PATENT ABSTRACTS OF JAPAN

(11)Publication number : **09-160492**

(43)Date of publication of application : **20.06.1997**

(51)Int.Cl. **G09C 1/00**
H04L 9/32

(21)Application number : **07-324908**

(22)Date of filing : **13.12.1995**

(71) Applicant : **MATSUSHITA ELECTRIC IND CO LTD**

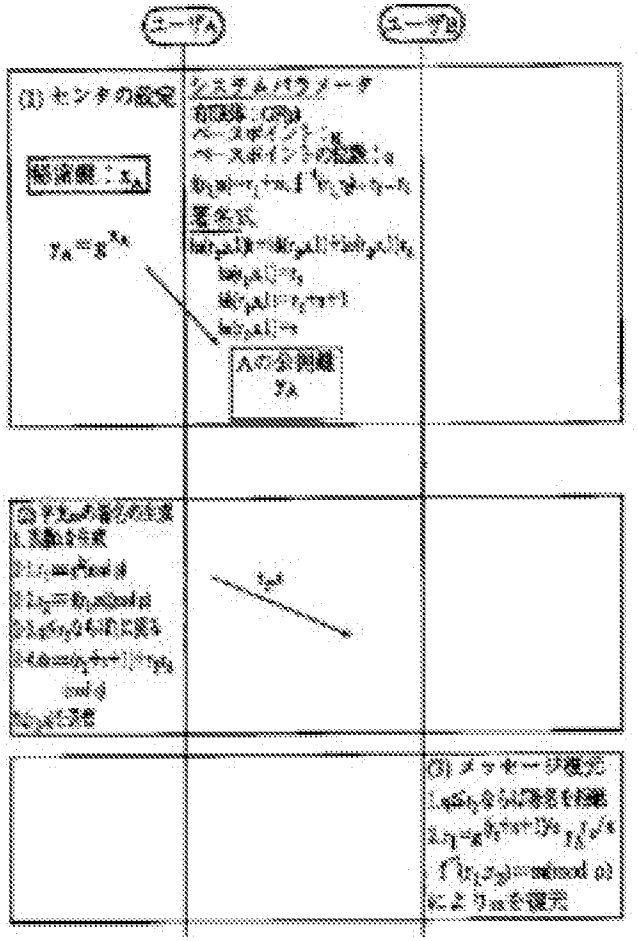
(72) Inventor : **MIYAJI MITSUKO**

(54) **SIGNATURE SYSTEM**

(57)Abstract:

PROBLEM TO BE SOLVED: To attain a signature system capable of restoring a message and having high safety.

SOLUTION: Mapping (f) from GF(p)×GF(p) to GF (p) satisfying following tow conditions to GF(p) is set up as a message masking expression. In the 1st condition, three variables (t), (j), (e) are not replaced by two algebraic expressions in f (gtyAj, myAe) and f(gtyAj, mge) in the case of GF(p) g, yA, m and Zq={0, 1,..., q-1} t, j, e. In the 2nd condition, the reverse image of r2=f(r1, m) is m=f-1(r1, r2). A signature expression is prepared by mapping ha, hb, hc from GF(p)×GF (p)×GF(p) satisfying following expressions [1], [2] to GF(p). Where, hb(r2', s, 1)-ha(r2', s, 1) ≠hb(rr2', ss, 1) when ha(r2', s, 1)=ha(rr2', ss, 1) and hc(r2', s, 1)=hc(rr2', ss, 1) [1] and hc (r2', s, 1)-ha(r2', s, 1)≠hc(rr2', ss, 1) when ha (r2', s, 1)=ha(rr2', ss, 1) and hb(r2', s, 1)=hb (rr2', ss, 1) [2].



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－160492

(43)公開日　平成９年(1997)６月20日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０９Ｃ	1/00	６４０	7259 -5J	Ｃ０９Ｃ	1/00	６４０Ｂ
			7259 -5J			６４０Ｄ
			7259 -5J			６４０Ｅ
Ｈ０４Ｌ	9/32			Ｈ０４Ｌ	9/00	６７５Ｂ

審査請求　未請求　請求項の数48　ＯＬ　（全 23 頁）

(21)出願番号　特願平7－324908

(22)出願日　平成７年(1995)12月13日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　宮地　充子
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　弁理士　中島　司朗

(54)【発明の名称】　署名方式

(57)【要約】

【課題】　メッセージ復元が可能かつ安全の高い署名方式を可能とする。

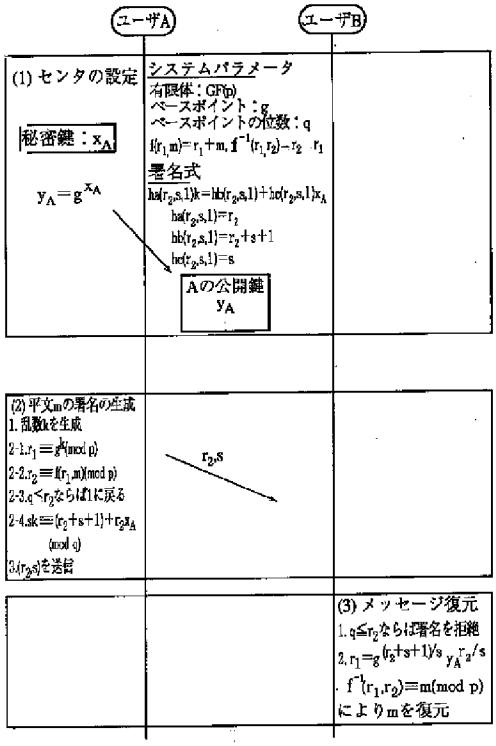
【解決手段】　以下の１、２を充たすGF(p) ×GF(p) からGF(p) への写像f をメッセージマスク式とする。

１：GF(p) ∋g, y_A , m, Zq= {0,1,…,q-1} ∋t, j, e に対し、$f(g^t y_A^j , m g^e)$ 及び$f(g^t yA^j , m g^e)$ において、３変数t,j,eが２個の代数式で置き換えられない。

2:同じく、$r_2=f(r_1,m)$の逆像は$m=f^{-1}(r_1,r_2)$ である以下の１、２を充たすGF(p) ×GF(p) ×GF(p) からGF(p) への写像ha, hb, hcにて署名式を作る。

1. $ha(r_2',s,1)=ha(rr_2',ss,1)$, $hc(r_2',s,1)=hc(rr_2',ss,1)$ のとき$hb(r_2',s,1)-ha(r_2',s,1)\neq hb(rr_2',ss,1)$

2. $ha(r_2',s,1)=ha(rr_2',ss,1)$, $hb(r_2',s,1)=hb(rr_2',ss,1)$ のとき$hc(r_2',s,1)-ha(r_2',s,1)\neq hc(rr_2',ss,1)$



【特許請求の範囲】

【請求項１】　ｐを素数とし、有限体GF(p) の元をg とし、その位数をq とし、

GF(p) 上定義される署名方式において、署名したい文をm ∈GF(p) とするとき、

k を署名者が任意にとる乱数とし、$r_1 \equiv g^k \pmod p$ を署名生成処理におけるコミットメントとし、GF(p) × GF(p) からGF(p) への写像をf とするとき、

r_1とm をf により変換したf(r_1, m)を用いて署名生成処理におけるメッセージ復元を可能にするメッセージマスク式を構成することを特徴としたメッセージ復元型署名方式。

【請求項２】　ｐを素数とし、r を正整数とし、有限体$GF(p^r)$ の元をg とし，その位数をq とし，$GF(p^r)$ 上定義される署名方式において，署名したい文をm ∈$GF(p^r)$とするとき，k を署名者が任意にとる乱数とし，$r_1 \equiv g^k \pmod p$ をコミットメントとし，$GF(p^r)$ ×$GF(p^r)$ から$GF(p^r)$ への写像をf_1とし，$GF(p^r)$ から有限環$Z_{p^r} = \{0,1,\cdots,p^{r-1}\}$ への写像をπとするとき，r_1とm をf1により変換し，この値を更にπを用いて変換したπ(f_1(r_1, m)) を用いて署名生成処理におけるメッセージ復元を可能にするメッセージマスク式を構成することを特徴としたメッセージ復元型署名方式。

【請求項３】　ｐを素数とし、有限体GF(p) 上定義された楕円曲線をE とし、

E(GF(p))の元をG とし、その位数をq とし、

E(GF(p))上定義される署名方式において、署名したい文をm ∈GF(p) とするとき、

k を署名者が任意にとる乱数とし、$R_1 = kG = (r_x, r_y)$ をコミットメントとし、

E(GF(p))×GF(p) からGF(p) への写像をFとするとき、R_1とm をにF より変換したF(R_1, m)を用いて署名生成処理におけるメッセージ復元を可能にするメッセージマスク式を構成することを特徴としたメッセージ復元型署名方式。

【請求項４】　ｐを素数とし、r を正整数とし、有限体$GF(p^r)$ 上定義された楕円曲線をE とし、

E($GF(p^r)$)の元をG とし、その位数をq とし、

E($GF(p^r)$)上定義される署名方式において、署名したい文をm ∈$GF(p^r)$ とするとき、

k を署名者が任意にとる乱数とし、$R_1 = kG = (r_x, r_y)$ をコミットメントとし、

E($GF(p^r)$)×$GF(p^r)$ から$GF(p^r)$ への写像をF1とするとし、$GF(p^r)$ から有限環Z_{p^r}への写像をπとするとき、R_1とm をF1により変換し、この値を更にπを用いて変換したπ(F_1(R_1, m)) を用いて署名生成処理におけるメッセージ復元を可能にするメッセージマスク式を構成することを特徴としたメッセージ復元型署名方式。

【請求項５】　写像f は、GF(p) ∋g, y_A 及び m, 並びにZq= {0,1,…,q-1} ∋t, j及びe に対し、

$f(g^t y_A^j, m y_A^e)$ 及び$f(g^t y_A^j, mg^e)$ において、３変数t,j,eが２個の代数式で非置換であることを特徴とした請求項１記載の離散対数問題を用いた署名方式。

【請求項６】　写像f は、$GF(p^r)$ ∋g, y_A 及びm,並びに Z_q= {0,1,…,q-1} ∋t, j及びe に対し、

$f_1(g^t y_A^j, m y_A^e)$ 及び$f_1(g^t y_A^j, mg^e)$ において、３変数t,j,e が２個の代数式で非置換であることを特徴とした請求項２記載の離散対数問題を用いた署名方式。

【請求項７】　写像F は、E(GF(p))∋G 及びY_A, GF(p)∋m,並びに Z_q = {0,1,…,q-1} ∋t, j及びe に対し、

$F(tG+jY_A, m \times x(eY_A))$及び$f(tG+jy_A, m \times x(eG))$ において、３変数t,j及び eが２個の代数式で非置換であることを特徴とした請求項３記載の離散対数問題を用いた署名方式。

【請求項８】　写像F1は、$E(GF(p^r))$∋G 及びY_A, $GF(p^r)$ ∋m,並びに Z_q = {0,1,…,q-1} ∋t, j及びe に対し、

$f(tG+jY_A, m \times x(eY_A))$及び$f(tG+jY_A, m \times x(eG))$ において、３変数t,j,e が２個の代数式で非置換であることを特徴とした請求項4 記載の離散対数問題を用いた署名方式。

【請求項９】　写像f は、GF(p) ∋r_1, r_2, m, g及びy_A に対し、r_2=f(r_1,m)の逆像をm=f^{-1}(r_1,r_2) で定義するとき、　任意の２変数関数φ，ψに対して

$f^{-1}(r_1/g, r_2) \neq \phi(m,g)$

及び$f^{-1}(r_1/y_A, r_2) \neq \psi(m,y_A)$

となることを特徴とした請求項１記載の離散対数問題を用いた署名方式。

【請求項１０】　写像f_1は、$GF(p^r)$ ∋r_1, r_2, m, g, y_A に対し、r_2=f_1(r_1,m) の逆像をm=f_1^{-1}(r_1,r_2) で定義するとき、　任意の２変数関数φ，ψに対して

$f_1^{-1}(r_1/g, r_2) \neq \phi(m,g)$

及び$f_1^{-1}(r_1/y_A, r_2) \neq \psi(m,y_A)$

となることを特徴とした請求項２記載の離散対数問題を用いた署名方式.

【請求項１１】　写像F は、E(GF(p))∋R_1, Y_A 及びG 並びにGF(p) ∋ m及びr_2に対し、r_2=f(R_1,m)の逆像をm=f^{-1}(R_1,r_2) で定義するとき、任意の２変数関数φ，ψに対して

$f^{-1}(R_1-G, r_2) \neq \phi(m,G)$

及び$f^{-1}(R_1-Y_A, r_2) \neq \psi(m,Y_A)$

となることを特徴とした請求項３記載の離散対数問題を用いた署名方式。

【請求項１２】　写像F_1は、$E(GF(p^r))$∋R_1, Y_A 及びG 並びに$GF(p^r)$ ∋m及びr_2に対し、r_2=f(R_1,m)の逆像をm=f^{-1}(R_1,r_2)で定義するとき、任意の２変数関数φ，ψに対して

$f^{-1}(R_1-G, r_2)\neq\phi(m,G)$
及び$f^{-1}(R_1-Y_A, r_2)\neq\psi(m,Y_A)$
となることを特徴とした請求項４記載の離散対数問題を用いた署名方式。
【請求項１３】　写像f は、(r, y)→r ＋y(GF(p) 上の加算）で定義されることを特徴とした請求項１記載のメッセージ復元型署名方式。
【請求項１４】　写像f1は、(r, y)→r ＋y(GF(p^r) 上の加算）で定義されることを特徴とした請求項２記載のメッセージ復元型署名方式。
【請求項１５】　写像F は、楕円曲線のｘ座標関数を用いて、(R, y)→x(R)＋y(GF(p) 上の加算）で定義されることを特徴とした請求項３記載のメッセージ復元型署名方式。
【請求項１６】　写像F_1は、楕円曲線のｘ座標関数を用いて、(R, y)→x(R)＋y(GF(p^r) 上の加算）で定義されることを特徴とした請求項４記載のメッセージ復元型署名方式。
【請求項１７】　写像πは、$\{\alpha_1, \alpha_2, \cdots, \alpha_r\}$をGF($p^r$) のGF(p)上の基底とするとき、GF(pr)の元$x=x_1\alpha_1+\cdots+x_r\alpha_r$ ($x_1, \cdots, x_r \in GF(p)$)に対して、
$\pi(x)=x_1+x_2p+\cdots+x_rp^{r-1}$
で定義されることを特徴とした請求項２、同４、同６、同８、同１０若しくは請求項１２記載のメッセージ復元型署名方式。
【請求項１８】　p を素数とし、有限体GF(p) の元をgとし、その位数をqとし、
GF(p) 上定義される署名方式において、署名者A の秘密鍵をx_A、公開鍵を$y_A=g^{x_A}$とし、署名したい文をm ∈GF(p) とするとき、k を署名者が任意にとる乱数とし、r_2をコミットメント$r_1=g^k$ とm により計算されるGF(p) の元とし、$r_2' \equiv r_2 \pmod q$ とし、
ha, hb, hcを有限環$Z_q \times Z_q \times Z_q$から$Z_q$ への写像とするとき、署名式を、
$ha(r_2',s,1)k \equiv hb(r_2',s,1) + hc(r_2',s,1)x_A \pmod q$
からs が計算できるように構成することを特徴としたメッセージ復元型署名方式。
【請求項１９】　p を素数とし、r を正整数とし、有限体GF(p^r) の元をgとし、その位数をq とし、
GF(p^r) 上定義される署名方式において、署名者A の秘密鍵をx_A、公開鍵を$y_A=g^{x_A}$とし、署名したい文をm ∈GF(p^r) とするとき、
k を署名者が任意にとる乱数とし、r_2をコミットメント$r_1=g^k$とm により計算される有限環Z_{p^r}の元とし、$r_2' \equiv r_2 \pmod q$ とし、
ha, hb, hcを有限環$Z_q \times Z_q \times Z_q$から$Z_q$ への写像とするとき、署名式を、
$ha(r_2',s,1)k \equiv hb(r_2',s,1) + hc(r_2',s,1)x_A \pmod q$
からs が計算できるように構成することを特徴としたメッセージ復元型署名方式。
【請求項２０】　p を素数とし、有限体GF(p) 上定義された楕円曲線をE とし、
E(GF(p))の元をG とし、その位数をq とし、
E(GF(p))上定義される署名方式において、署名したい文をm ∈GF(p) とするとき、
k を署名者が任意にとる乱数とし、r_2をコミットメント$R_1=kG$ とm により計算されるGF(p) の元とし、$r_2' \equiv r_2 \pmod q$ とし、
ha, hb, hcを有限環$Z_q \times Z_q \times Z_q$から$Z_q$ への写像とするとき、署名式を、
$ha(r_2',s,1)k \equiv hb(r_2,s,1) + hc(r_2',s,1)x_A \pmod q$
からs が計算できるように構成することを特徴としたメッセージ復元型署名方式。
【請求項２１】　p を素数とし、r を正整数とし、有限体GF(p^r) 上定義された楕円曲線をE とし、
E(GF(p^r))の元をG とし、その位数をq とし、
E(GF(p^r))上定義される署名方式において、署名したい文をm ∈GF(p^r) するとき、
k を署名者が任意にとる乱数とし、r_2をコミットメント$R_1=kG$ とm により計算される有限環Z_{p^r}の元とし、$r_2' \equiv r_2 \pmod q$ とし、
ha, hb, hcを有限環$Z_q \times Z_q \times Z_q$から$Z_q$ への写像とするとき、署名式を、
$ha(r_2',s,1)k \equiv hb(r_2',s,1) + hc(r_2',s,1)x_A \pmod q$
からs が計算できるように構成することを特徴としたメッセージ復元型署名方式。
【請求項２２】　写像ha,hb, hc は、r_2',s をZ_q の元とするとき、別途予め固定された所定値を除く任意のZ_q の元rr_2', ssに対して、次の二つの条件
1. $ha(r_2',s,1)=ha(rr_2',ss,1)$, $hc(r_2',s,1)=hc(rr_2',ss,1)$ のとき
$hb(r_2',s,1)-ha(r_2',s,1)\neq hb(rr_2',ss,1)$
2. $ha(r_2',s,1)=ha(rr_2',ss,1)$, $hb(r_2',s,1)=hb(rr_2',ss,1)$ のとき
$hc(r_2',s,1)-ha(r_2',s,1)\neq hc(rr_2',ss,1)$
を満足することを特徴とした請求項１８、同１９、同２０若しくは請求項２１記載の離散対数問題を用いた署名方式。
【請求項２３】　写像ha,hb,hcは、
$ha(r_2',s,1)=r2'$, $hc(r_2',s,1)=s$とし、
$hb(r_2',s,1)$ は、
$r_2'=rr_2'$, s=ssのとき、$hb(r_2',s,1)=hb(rr_2',ss,1)$ 、
$r_2'=rr_2'$, $hb(r_2',s,1)=hb(rr_2',ss,1)$ のとき、s=ss、
hb(0, 0, 1) ≠0,
を満たすことを特徴とした請求項２２記載のメッセージ復元型署名方式。
【請求項２４】　写像ha,hb,hcは、

ha(r_2',s,1)=s, hc(r_2',s,1)=r_2'とし、
hb(r_2',s,1) は、
s=ss, r_2'=rr$_2$', のとき、hb(r_2',s,1)=hb(rr$_2$',ss,1)
、
s=ss, hb(r_2',s,1)=hb(rr$_2$',ss,1) のとき、r_2'=rr$_2$'、
hb(0, 0, 1) ≠0
を満たすことを特徴とした請求項２２記載のメッセージ復元型署名方式。
【請求項２５】　写像ha,hb,hcは、
ha(r_2',s,1)=s, hb(r_2',s,1)=r_2'とし、
hc(r_2',s,1) は、
r_2'=rr$_2$', s=ssのとき、hc(r_2',s,1)=hc(rr$_2$',ss,1) 、
s=ss, hc(r_2',s,1)=hc(rr$_2$',ss,1) のとき、r_2'=rr$_2$'
hc(0, 0, 1) ≠0
を満たすことを特徴とした請求項２２記載のメッセージ復元型署名方式。
【請求項２６】　写像ha,hb,hcは、
ha(r_2',s,1)=r$_2$', hb(r_2',s,1)=sとし、
hc(r_2',s,1) は、
r_2'=rr$_2$', s=ssのとき、hc(r_2',s,1)=hc(rr$_2$',ss,1) 、
r_2'=rr$_2$', hc(r_2',s,1)=hc(rr$_2$',ss,1) のとき、s=ss、
hc(0, 0, 1) ≠0
を満たすことを特徴とした請求項２２記載のメッセージ復元型署名方式。
【請求項２７】　写像ha,hb,hcは、
hc(r_2',s,1)=s, hb(r_2',s,1)=r_2'とし、
ha(r_2',s,1) は、
r_2'=rr$_2$', ha(r_2',s,1)=ha(rr$_2$',ss,1) のとき、s=ss、
s=ss, ha(r_2',s,1)=ha(rr$_2$',ss,1) のとき、r_2'=rr$_2$'、
ha(0,0,1) ≠0
を満たすことを特徴とした請求項２２記載のメッセージ復元型署名方式。
【請求項２８】　写像ha,hb,hcは、
hc(r_2',s,1)=r$_2$', hb(r_2',s,1)=sとし、
ha(r_2',s,1) は、
r_2'=rr$_2$', ha(r_2',s,1)=ha(rr$_2$',ss,1) のとき、s=ss、
s=ss, ha(r_2',s,1)=ha(rr$_2$',ss,1)のとき、r_2'=rr$_2$'、
ha(0,0,1) ≠0
を満たすことを特徴とした請求項２２記載のメッセージ復元型署名方式。
【請求項２９】　写像hb(r_2',s,1) は、
hb(r_2',s,1)=r_2' ＋s ＋1
で定義されることを特徴とした請求項２３若しくは請求項２４記載のメッセージ復元型署名方式。
【請求項３０】　写像hb(r_2',s,1) は、
hb(r_2',s,1)=r_2' ×s ＋1
で定義されることを特徴とした請求項２３若しくは請求項２４記載のメッセージ復元型署名方式。
【請求項３１】　写像hc(r_2',s,1) は、
hc(r_2',s,1)=r_2' ＋s ＋1
で定義されることを特徴とした請求項２５若しくは請求項２６記載のメッセージ復元型署名方式。
【請求項３２】　写像hc(r_2',s,1) は、
hc(r_2',s,1)=r_2' ×s ＋1
で定義されることを特徴とした請求項２５若しくは請求項２６記載のメッセージ復元型署名方式。
【請求項３３】　写像ha(r_2',s,1) は、ha(r_2',s,1)=0
となる解(r_2',s) がビットの多項式で定まる有限時間で確定できることを特徴とした請求項２７若しくは請求項２８記載のメッセージ復元型署名方式。
【請求項３４】　乱数k を、メッセージマスク式で計算されるr$_2$と署名式で計算されるs に対して、
ha(r_2',s,1) ≠0
であるように取ってくることを特徴とした請求項３３記載のメッセージ復元型署名方式。
【請求項３５】　写像ha(r_2',s,1) は、
ha(r_2',s,1)=r_2'+s+1 であることを特徴とした請求項３４記載のメッセージ復元型署名方式。
【請求項３６】　写像ha(r_2',s,1) は、
ha(r_2',s,1)=r_2' ×s ＋1 であることを特徴とした請求項３４記載のメッセージ復元型署名方式。
【請求項３７】　p を素数とし、q の１／４以上となる正整数とし、有限体GF(p) の位数がq となる元をg とし、
GF(p) 上定義される署名方式において、署名したい文をm ∈GF(p) とするとき、乱数k を、コミットメントr_1＝g^k とm により構成されるGF(p) の元r_2が、
０＜ r_2 ＜q となるようにとり、
上記範囲を限定されたr_2を署名式に用いることを特徴としたメッセージ復元型署名方式。
【請求項３８】　p を素数とし、r を正整数とし、q をp と大きさがほぼ同じである，すなわちp ～q となる正整数とし、有限体GF(p^r) の位数がq となる元をg とし、
GF(p^r) 上定義される署名方式において、署名したい文をm ∈GF(p^r) とするとき、乱数k を、コミットメントr_1＝g^k とm により構成されるZ$_{p^r}$= {0,1,…,p^{r-1} } の元r_2が、
０＜ r_2 ＜q となるようにとり、
上記範囲を限定されたr_2を署名式に用いることを特徴としたメッセージ復元型署名方式。
【請求項３９】　p を素数とし、有限体GF(p) 上定義された楕円曲線をE とし、
E(GF(p))の元をG とし、その位数をq とし、
E(GF(p))上定義される署名方式において、署名したい文をm ∈GF(p) とするとき、乱数k を、コミットメントr_1＝g^k とm により構成されるGF(p) の元r_2が、
０＜ r_2 ＜q となるようにとり、
上記範囲を限定されたr_2を署名式に用いることを特徴としたメッセージ復元型署名方式。

【請求項４０】　ｐを素数とし、ｒを正整数とし、有限体GF(p^r)上定義された楕円曲線をEとし、
E(GF(p^r))の元をGとし、その位数をｑとし、
E(GF(p^r))上定義される署名方式において、署名したい文をｍ∈GF(p^r)とするとき、乱数ｋを、コミットメント$r_1=g^k$とｍにより構成されるZ_{p^r}＝｛0,1,…,p^{r-1}｝の元r_2が、
０＜　r_2　＜ｑとなるようにとり、
上記範囲を限定されたr_2を署名式に用いることを特徴としたメッセージ復元型署名方式。
【請求項４１】　楕円曲線Eは、
元の個数がｐとなるGF(p)上の楕円曲線を用いることを特徴とした請求項３９記載の署名方式。
【請求項４２】　署名したい文ｍに対し、ｍのハッシュ関数値hash(ｍ)をｍの代わりに用いることを特徴とした請求項１、同２、同３、同４、同１８、同１９、同２０、同２１、同３７、同３８、同３９若しくは請求項４０記載の署名方式。
【請求項４３】　ｐを素数とし、有限体GF(p)の元をｇとし、その位数をｑとし、
GF(p)上定義される署名方式において、署名者Ａの秘密鍵をx_A、公開鍵を$y_A=g^{x_A}$とし、署名したい文をｍ∈GF(p)とするとき、
ｋを署名者が任意にとる乱数とし、コミットメント$r_1=g^k$とし、
$r_1'\equiv r_1 \pmod q$, $m'\equiv m \pmod q$とし、
ha, hb, hcを有限環$Z_q\times Z_q\times Z_q$からZ_qへの写像とするとき、署名式を、
$ha(r_1',s,m')k \equiv hb(r_1',s,m') + hc(r_1',s,m')x_A \pmod q$
からｓが計算できるように構成することを特徴とした署名方式。
【請求項４４】　ｐを素数とし、ｒを正整数とし、有限体GF(p^r)の元をｇとし、その位数をｑとし、
GF(p^r)上定義される署名方式において、署名者Ａの秘密鍵をx_A、公開鍵を$y_A=g^{x_A}$とし、署名したい文をｍ∈GF(p^r)とするとき、
ｋを署名者が任意にとる乱数とし、コミットメント$r_1=g^k$とし、GF(p^r)から有限環Z_{p^r}への写像をπとするとき、
$r_1'\equiv \pi(r_1) \pmod q$, $m'\equiv \pi(m) \pmod q$とし、
ha, hb, hcを有限環$Z_q\times Z_q\times Z_q$からZ_qへの写像とするとき、署名式を、
$ha(r_1',s,m')k \equiv hb(r_1',s,m') + hc(r_1',s,m')x_A \pmod q$
からｓが計算できるように構成することを特徴とした署名方式。
【請求項４５】　ｐを素数とし、有限体GF(p)上定義された楕円曲線をEとし、
E(GF(p))の元をGとし、その位数をｑとし、
E(GF(p))上定義される署名方式において、署名したい文をｍ∈GF(p)とするとき、
ｋを署名者が任意にとる乱数とし、コミットメント$R_1=kG$とし、E(GF(p))からGF(p)への写像をρとするとき、
$r1'\equiv \rho(R_1) \pmod q$, $m'\equiv m \pmod q$とし、
ha, hb, hcを有限環$Z_q\times Z_q\times Z_q$からZ_qへの写像とするとき、署名式を、
$ha(r_1',s,m')k \equiv hb(r_1',s,m') + hc(r_1',s,m')x_A \pmod q$
からｓが計算できるように構成することを特徴とした署名方式。
【請求項４６】　ｐを素数とし、ｒを正整数とし、有限体GF(p^r)上定義された楕円曲線をEとし、
E(GF(p^r))の元をGとし、その位数をｑとし、
E(GF(p^r))上定義される署名方式において、署名したい文をｍ∈GF(p^r)とするとき、
ｋを署名者が任意にとる乱数とし、コミットメント$R_1=kG$とし、E(GF(p^r))からGF(p^r)への写像をρとするとし、GF(p^r)から有限環Z_{p^r}＝｛0,1,…,p^{r-1}｝への写像をπとするとき、
$r_1'\equiv \pi(\rho(R_1)) \pmod q$, $m'\equiv \pi(m) \pmod q$とし、
ha, hb, hcを有限環$Z_q\times Z_q\times Z_q$からZ_qへの写像とするとき、署名式を、
$ha(r_1',s,m')k \equiv hb(r_1',s,m') + hc(r_1',s,m')x_A \pmod q$
からｓが計算できるように構成することを特徴とした署名方式。
【請求項４７】　写像ρは、楕円曲線のｘ座標若しくはｙ座標関数を用いて、R→x(R)若しくはR→ｙ（Ｒ）で定義されることを特徴とした請求項４５若しくは請求項４６記載のメッセージ復元型署名方式。
【請求項４８】　写像πは、｛α_1，α_2，…，α_r｝をGF(p^r)のGF(p)上の基底とするとき、GF(p^r)の元$x=x_1\alpha_1+\cdots+x_r\alpha_r$（$x_1$，…，$x_r\in$GF(p)）に対して、
$\pi(x)=x_1+x_2p+\cdots+x_r p^{r-1}$
で定義されることを特徴とした請求項４４及び請求項４６記載のメッセージ復元型署名方式。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、情報の通信保持技術に関し、特に、離散対数問題を安全性の根拠として用いるデジタル署名技術に関する。
【０００２】
【従来の技術】
（発明の技術的背景）本願発明に直接関係する技術は、我国では未だ必ずしも一般に周知とは言いがたいので、まず、間接的に関係する技術も含めて公開ディジタル通信網を使用した暗号通信技術を広く一般的に説明する。

なお、この秘密通信方式等の一般技術については、わが国では、学術書としては池野信一、小山謙二著「現代暗号理論」　電子通信学会発行　１９８６年、一般向けとしては、一松　信著「暗号の数理」　講談社刊１９８０年に詳しい。

【０００３】近年、一般に公開されたディジタル通信回線網を使用して相互に通信を行ったり、有料で放送番組を提供したりすることがさかんになってきている。ところで、一般に公開された通信回線網を使用する場合、第三者による盗聴や詐称、あるいは送信者による送信先の間違いを完全に防止することは困難である。このため、秘密通信方式並びに署名及び認証方式と呼ばれる通信方式が重要なものとなっている。ここに、秘密通信方式とは、特定の通信相手以外に通信内容を漏らすことなく通信を行う方式である。また署名及び認証通信方式とは、通信相手に通信内容の正当性を示したり、本人であることを証明する通信方式である。さて、この秘密通信及び署名、認証通信の方式には、公開鍵暗号とよばれる数値を利用した方式がある。そして、この公開鍵暗号による方式は、ＮＴＴ等の公開ディジタル通信網により、国内外の多数の相手と通信を行う等のごとく通信相手が多数、しかも通信者が相互に暗号技術について本来的に素人であるとき、通信相手ごとに異なる暗号鍵を容易に管理するための方式であり、現在では多数の通信相手と通信を行うのに不可欠な基盤技術とされている。

【０００４】以下、この暗号通信技術の基本的原理と手順と特徴を２、３簡単に説明する。

（１）有限体上の離散対数問題を使用した秘密通信方式。

なお、これはニイルコブリッツ著　”ア　コウス　イン　ナンバア　セオリイアンド　クリプトグラヒイ”(Neal koblitz , ”A Course in Number Theoryand Cryptography ”,Springer-Verlag,1987)に詳しく述べられている。

（原理）ｐを素数、ｇをその一の原始根、ｕを任意の自然数、αをｇのｕ乗のｐを法とする剰余とする。すなわち、$g^u \equiv \alpha$（ｍｏｄ　ｐ）とする。この場合、ｇとｐとｕを与えられたときにαを求めるのは容易である。しかし、ｐが１４０桁程度の素数となると、大型計算機の発達した今日でも、ｇとｐとαからｕを求めるのは困難である。これは丁度、２つの素数ｒとｓがあるときｒとｓからその積を求めるのは容易であるが、ｒとｓが各１４０桁程度となれば、積は２８０桁となるため、これから素因数分解によりｒとｓを求めるのは困難なことに似る。

（２）楕円曲線上の離散対数問題を使用した秘密通信方式。

【０００５】しかしながら、近年の大型計算機の発達を背景にして、数学の理論（類体論の高次相互律、分解法則等）を使用して、ｇとｐとαとから比較的少ない計算量でｕを求める方法が種々開発されつつある。その対策の一としては、素数ｐを１４０桁程度のものでなく２００桁等充分に大きいものとすることがあげられる。ただし、この場合には、桁数が大きいだけに、送受信に際して必要な計算の絶対量が多くなる等の不都合が生じえる。

【０００６】これらのため、楕円曲線を使用した秘密通信方式が開発された。

（原理）次にＥ｛ＧＦ（ｑ）｝の性質、すなわち秘密通信の根拠の原理について説明する。Ｅ｛ＧＦ（ｑ）｝の位数が大きな素数で割れる元ＢＰをベースポイント、ｄは任意の自然数とする。このとき、ＢＰとｄとからｄ・ＢＰを計算する（ＢＰをｄ回加える）のは容易である。しかし、Ｅ｛ＧＦ（ｑ）｝の与えられた元ＱとＢＰに対して、

Ｑ＝ｄ・ＢＰ

となる自然数ｄが存在するならばｄを求めよという問題は、計算機の発達した今日でもＢＰやｑ等が３０桁程度の自然数となるならば困難である。なお、ここにＢＰは、ｐを法とする有限体ＧＦ（ｐ）上でのｇに相当する役を担うものである。

【０００７】以上で、暗号通信の一般技術の概略説明は終了する。

（３）署名、認証通信

次に、本願発明に関係する技術たる署名、認証通信について説明する。有限体上の離散対数問題におけるユーザＵとユーザＶの共有鍵k_{uv}を使用しての秘密通信を例にとるならば、ユーザＵあるいはユーザＶにとって、一番最初に確かに相手がユーザＶあるいはユーザＵであることを認証すること、すなわち第三者による詐称を排除する必要がある。

【０００８】この場合、ユーザＵとユーザＶとが面談、書留め郵便等により直接確認する手段もあるが、国際間はもとより国内の通信においても煩雑となる。この解決手段として、通信網による公開された数値情報を利用して署名、認署を行う技術が開発されている。以下この技術について、２、３紹介する。

（通信網提供者による署名認署）最初、システム初期設定として、通信網提供者が、その秘密鍵Ｘと、端末の秘密鍵を生成するためのある秘密鍵生成関数Ｓを保有し、端末の公開鍵を生成するための所定の公開鍵生成関数Ｐと、所定の一方向性関数Ｆと、秘密鍵Ｘを一方向性関数Ｆに入力したときの出力値Ｙ＝Ｆ（Ｘ）とを端末情報発行センターの公開情報として公開ディジタル通信網を使用する各ユーザに通知する。

【０００９】次に、送信に際して、送信者の正当性の証明を欲するユーザＵが、その端末固有の識別情報ID_uと、自分で作成した秘密鍵をもとに作成した公開値をセンターに通知し、その登録を請求する。なお、秘密鍵ｘと公開値との間には、ｘ＝Ｓ（ｘ，ｙ，ｋ，ID_u）の

関係がある。ここに、ｙ＝Ｆ（ｋ）、またｋは乱数値である。

【００１０】ユーザＵからの請求を受けた通信網提供者が、ユーザＵの公開値y_uを他のユーザに公開する。すなわち、ユーザＵは、検証用公開鍵として、その秘密鍵ｘを前記一方向性関数Ｆに入力したときの出力値y_u＝Ｆ（ｘ）を生成し、送信相手となるユーザＶに対して、自分の公開情報として、その公開値ｙと識別情報ＩＤｕとy_uを、公開ディジタル通信網を介して転送する。

【００１１】ユーザＶは、ユーザＵからその端末公開情報の転送を受けると、ユーザＵの公開鍵として、網提供者の公開情報Ｙと、ユーザＵの公開値ｙと、その識別情報ＩＤｕとを公開鍵生成関数Ｐに入力したときの出力値Ｃ＝Ｐ（Ｙ，ｙ，ＩＤｕ）を生成するこの上で、生成されたユーザＵの公開鍵Ｃと前記検証用公開鍵y_uを比較し、一致するか否かを確認する。一致したならば、確かに送信者はユーザＵであると認める。

【００１２】これにより、ユーザＶは網提供者の発行した公開値Ｙを使用してユーザＵから送信されてきた公開鍵を入手しえ、ひいては確かにユーザＵから送られてきたものと認められる。以上の概略の手順、必要な構成を図２に示す。なお、認証は必ずしも通信網提供者とは限らないのも勿論である。

【００１３】次に、具体的な関数式、関数値としての各鍵の値等としては、Ｙは、式$Y \equiv F(X) \equiv g^x \pmod p$等が用いられ、ｋｕは乱数発生機により計算され、Ｙｕは、式$Yu \equiv g \wedge ku \pmod p$により計算し、ｘｕは、式$xu \equiv S(X, yu, ku, IDu) \equiv X \times yu + ku \times IDu \pmod \phi$、（ここに、φはｐのオイラー関数値）等により計算され、Ｐｕは、式$Pu = P(Y, yu, IDu) \equiv (Y \wedge yu) \times (yu \wedge IDu) \pmod p$等により計算される。なおここに、オイラーの関数φとは、整数である変数の値より小さいかつその変数と互に素な整数の個数をいい、例えばφ（ｐ）＝ｐ－１，φ（６）＝２（注、１と５），φ（１０）＝４（注、１、３、７、９）である。また、任意の互に素な２つの整数ｕとｖの間には、$u \wedge \phi(v) - 1 \equiv 0 \pmod v$という関係が常に成立する。例えば、$3^{\phi(10)} - 1 = 3^4 - 1 = 80 \equiv 0 \pmod{10}$である。また、素数ｐについては、必ず$n^p - 1 \equiv 0 \pmod p$となり、この対偶として、任意の整数ｍについて、何か１つの整数ｎに対して$n^m - 1 \equiv 0 \pmod n$が成立しないならば、ｍは素数でないことがわかる。

（第３者による署名、認証）次に、ユーザＵとユーザＶとの認証に第三のユーザＷを介する方式ものもある。この場合には、ユーザＵとユーザＷ、ユーザＶとユーザＷとは相互に認証が必要であるが、ユーザＵとユーザＶとの直接の認署は不要となる。そしてこれは、銀行（ユーザＷに相当）を介しての金銭取引等で重要である。

【００１４】なお、これら署名、認証の内容、方式については別途本願出願人が、特願平２－３２４４７９号「公開鍵生成方法及び装置」等にて開示し、また前掲の現代暗号理論にても種々記載されている周知技術であるため、これ以上の説明は省略する。

（４）メッセージ復元署名

次に、署名、認署についての技術の一として、本願発明に直接関係するメッセージ復元型署名について説明する。

【００１５】１９９３年にNyberg-Rueppelにより離散対数問題に安全性の根拠をおくメッセージ復元型署名が発表された。以下に離散対数問題を用いたメッセージ復元型署名のひとつについて述べる。これについて詳しくは、Nyberg and Rueppel,"A new signature scheme based on the DSA giving message recovery",1st ACM Conf. on Comp. and Comm. Security, 1993 を参照されたい。

（メッセージ復元型署名の従来例）図３は、従来技術としての、上記Nyberg-Rueppel方式におけるメッセージ復元型署名の手順及び構成を示すものである。

【００１６】以下、本図を参照しながら従来例の手順を説明する。

（１）センターによる初期設定

ｐ を素数、GF(p) の元をｇ としその位数をｑ とする。センターは、システムパラメータとしてｐ，ｑ，ｇ を全ユーザ、すなわち公開ディジタル通信網に接続された全端末に公開する。

（２）ユーザＡによる秘密鍵の生成と公開鍵の登録要求の発生。

【００１７】署名通信を希望するユーザＡが、その端末情報とを作成し、これを使用してしての秘密鍵と対応する公開鍵も作成し、公開鍵の登録をセンターに要求する。このためユーザＡは、乱数x_Aを発生させ、これを自分の秘密鍵x_Aとし、対応する公開鍵を$y_A \equiv g x_A \pmod P$により求める。更にセンターを経由して、全ユーザにユーザＡの公開鍵y_Aを公開する。

（３）ユーザＡによる署名の生成及び送信。

【００１８】ユーザＢに署名、認署通信の発信を行うユーザＡは、以下の処理を行う。

１．乱数ｋを生成させる。

２．次いで、以下の演算を行う。なお、ここにｍは通信文である。

$r_1 \equiv g^k \pmod p$

$r_2 \equiv m / r_1 \pmod p \cdots (a)$

$r_2' \equiv r_2 \pmod q$

$s \equiv k - r_2' x_A \pmod q \cdots (b)$ を計算する。

【００１９】３．ユーザＡは(r_2', s)を、ユーザＢに送信する。

（４）ユーザＢによる受信したメッセージの復元

ユーザＢは、以下の式を計算することにより、メッセー

ジm を復元する。

１．$g^s y_A^{r2'} r_2 \equiv m \pmod p$

ここで、上記r_1はコミットメントと呼ばれ、(a) はメッセージマスク式，(b)は署名式と呼ばれる。

【００２０】上記従来例は、従来不可能であった離散対数問題に基づくメッセージ復元型署名を可能にする。また署名式(b) は以下のように６（＝３！）種類の式に一般化される。

$ak = b + cx_A \pmod q$，(a,b,c)=(1,r_2',s)の置換…(b')

【００２１】

【発明が解決しようとする課題】しかしながら、この従来例のメッセージ復元型署名に対しては、式が（ａ）と（ｂ）が簡単なため変形が容易であり、例えばy_A 及ぶｇのべき乗並びにｍについての掛け算の式が、３変数より２変数の式に置換しえる等のため近年幾つかの攻撃recovery-equation attack using g and yA, signature-equation attackusing g and yA,and homomorphism attack （各「ｇとy_A を使用した再生攻撃」、「ｇとy_A を使用した署名攻撃」及び「準同型攻撃（選択平文攻撃）」が発表された。これについて詳しくは、宮地　充子、「メッセージ復元型署名の弱点１」、電子情報通信学会、情報セキュリティ研究会、１９９５，７月及びNybergand Rueppel, "A new signature scheme based on the DSA giving message recovery", 1st ACM Conf. on Comp. and Comm.Security, 1993及びNyberg andRueppel, "Message recovery for signature schemes based on the discretelogarithm problem", Advances in cryptology-Proceedings of Eurocrypt'94,Lecture Notes in Computer Science, 950(1995), Springer-Varlag, 182-193を参照されたい。なお、参考までにその攻撃の１つを図４に示す。

【００２２】これらに加えて、次に述べる冗長性を利用した攻撃（redundancy attack）が存在する。署名通信等では、解読の困難性からはｐ、ｑは大きい程好ましいが、必要な演算が少なくて済む等の面からは小さい方が好ましい。このかねあいから実際的にはｐは５１２ビット、１０２４ビット程度の素数が使用されるが、ｑは１６０ビット程度の数が使用される。この場合、上記$r_2' \equiv r_2 \pmod q$ の式では、ｐ以下でr_2' 以外にこの式を充たす数rr_2 が存在しうる。本読解はこれを利用したものである。

【００２３】今、偽造者が一つの署名(r_2,s)を手にいれたとき、容易にこの署名文ｍが復元できるが、このとき

$rr_2=r_2'+q \pmod p$　（ここに、rr_2 とはr_2 の偽を意味する。）

$mm=rr_2\times(m/r_2)$　（ここに、ｍｍとは、ｍの偽を意味する）

を計算し、第三者に(rr_2,s) を送信する。これを受け取った第三者は、Ａの公開鍵を用いて従来例に示した復元方法でｍｍを復元し、Ａから送られたと思ってしまう。この結果、偽造者はＡになりすますことができる。

【００２４】参考までに、この攻撃の概要を図５に示す。なお、本図の「チルダー」は偽造者が署名を生成することを意味する。これら６つの攻撃により、上記従来例のメッセージ復元型署名方式は、署名式の形によらず、ある文の署名の偽造が一組の文と署名のペアを得るだけで可能になり、安全な方式とはいえなくなった。

【００２５】そして、これらのことは、楕円曲線を使用した場合にもあてはまる。以上説明してきたように最近になってメッセージ復元型署名は、その解読方法が考案され、このためこの署名は安全でないことがわかった。この解読方法は従来の署名（メッセージを復元できない署名）には適応できないことがわかっている。しかし、メッセージ復元性は有用な性質であり、この性質を保持しつつ解読が回避できることが望ましいといって、あまり複雑な署名式、メッセージマスク式を採用したりするのは、必要な計算量の減少を図るという面から好ましくない。

【００２６】本発明は、この従来例における問題点を鑑みてなされたもので、メッセージ復元性を保ちながら、提案された各種の解読に対して強い、しかも必要な計算量の少ないメッセージ復元型署名方式を提供することを目的とする。

【００２７】

【課題を解決するための手段】本発明における署名方式は、ｐ を素数とし、有限体GF(p) の元をｇ とし、その位数をｑ とし、GF(p) 上定義される署名方式において、署名者A の秘密鍵をx_A、公開鍵を$y_A=g^{xA}$とし、署名したい文をｍ ∈GF(p) とするとき、ｋ を署名者が任意にとる乱数とし、コミットメント$r_1=g^k$とし、$r_1' \equiv r_1 \pmod q$，$m' \equiv m \pmod q$ とし、ha，hb，hcを有限環$Z_q \times Z_q \times Z_q$ からZ_q への写像とするとき、署名式を、$ha(r_1',s,m')k \equiv hb(r_1',s,m') + hc(r_1',s,m')x_A \pmod q$からｓ が計算できるように構成している。これにより、各種の攻撃を回避する。

【００２８】また、本発明におけるメッセージ復元を可能にするメッセージマスク式を使用したメッセージ復元型署名方式は、メッセージマスク式として、ｐ を素数とし、有限体GF(p) の元をｇ とし、その位数をｑ とし、GF(p) 上定義される署名方式において、署名したい文をｍ∈GF(p) とするとき、ｋ を署名者が任意にとる乱数とし、$r_1 \equiv g^k \pmod p$ を署名生成処理におけるコミットメントとし、GF(p) ×GF(p) からGF(p) への写像をｆとするとき、r_1とｍ をｆ により変換したf(r_1，ｍ)を用いる。これにより、各種の攻撃を回避する。

【００２９】また、本発明における署名方式、メッセージ復元型署名方式は、ＥＧ（p^r），Ｅ（ＧＦ（ｐ））、Ｅ（ＧＦ（p^r）上でもなされる。

【００３０】

【発明の実施の形態】従来技術で記載した目的を達成するため、請求項１の発明では、特にGF(p) 上のメッセージ復元型署名において、p を素数とし、有限体GF(p) の元をg とし、その位数をq とし、GF(p) 上定義される署名方式において、署名したい文をm ∈GF(p) とするとき、k を署名者が任意にとる乱数とし、$r_1 = g^k$ を署名生成処理におけるコミットメントとし、GF(p) ×GF(p) からGF(p) への写像をf とするとき、r_1とm をf により変換したf(r_1, m)を用いて署名生成処理におけるメッセージ復元を可能にすることを特徴としている。

【００３１】請求項２の発明では、特にGF(p^r) 上のメッセージ復元型署名において、p を素数とし、r を正整数とし、有限体GF(p^r) の元をg とし，その位数をq とし、GF(p^r) 上定義される署名方式において、署名したい文をm ∈GF(p^r) とするとき、k を署名者が任意にとる乱数とし，$r_1 = g^k$ をコミットメントとし、GF(p^r) ×GF(p^r) からGF(p^r) への写像をf_1とし，GF(p^r) から有限環$Z_{p^r} = \{0,1,\cdots,p^{r-1}\}$ への写像をπとするとき、r_1とm をf_1により変換し，この値を更にπを用いて変換したπ(f_1(r_1, m)) を用いて署名生成処理におけるメッセージ復元を可能にすることを特徴としている。

【００３２】請求項３の発明では、特にGF(p) 上のメッセージ復元型署名において、p を素数とし、有限体GF(p) 上定義された楕円曲線をE とし、E(GF(p))の元をGとし、その位数をq とし、E(GF(p))上定義される署名方式において、署名したい文をm∈GF(p) とするとき、k を署名者が任意にとる乱数とし、$R_1 = kG = (r_x, ry)$ をコミットメントとし、E(GF(p))×GF(p) からGF(p) への写像をFとするとき、R_1とm をにF より変換したF(R_1, m)を用いて署名生成処理におけるメッセージ復元を可能にすることを特徴としている。

【００３３】請求項４の発明では、特にE(GF(p^r))上のメッセージ復元型署名において、pを素数とし、r を正整数とし、有限体GF(p^r) 上定義された楕円曲線をE とし、E(GF(p^r))の元をG とし、その位数をq とし、E(GF(p^r))上定義される署名方式において、署名したい文をm ∈GF(p^r) とするとき、k を署名者が任意にとる乱数とし、$R_1 = kG = (r_x, r_y)$ をコミットメントとし、E(GF(p^r))×GF(p^r) からGF(p^r) への写像をF_1とするとし、GF(p^r) から有限環Z_{p^r}への写像をπとするとき、R_1とm をF_1により変換し、この値を更にπを用いて変換したπ(F_1(R_1, m)) を用いて署名生成処理におけるメッセージ復元を可能にすることを特徴としている。

【００３４】請求項５の発明では、特にメッセージ復元型署名の上のrecovery-equation 攻撃を回避するため、写像f は、GF(p) ∋g, y_A 及び m, 並びにZq= {0,1, …,q-1} ∋t, j及びe に対し、f($g^t y_A^j$, my_A^e) 及びf($g^t y_A^j$, mg^e) において、３変数t,j,e が２個の代数式で非置換である（置き換えられない）ことを特徴としている。

【００３５】請求項６の発明では、特にメッセージ復元型署名の上のrecovery-equation 攻撃を回避するため、写像f は、GF(p^r) ∋g, y_A 及びm 並びにZ$_q$ = {0,1, …,q-1} ∋t, j及びe に対し、$f_1(g^t y_A^j, my_A^e)$ 及び$f_1(g^t y_A^j, mg^e)$ において、３変数t,j,e が２個の代数式で非置換である（置き換えられない）ことを特徴としている。

【００３６】請求項７の発明では、特にメッセージ復元型署名の上のrecovery-equation 攻撃を回避するため、写像F は、E(GF(p))∋G 及びY_A , GF(p)∋m 並びにZ$_q$ = {0,1,…,q-1} ∋t, j及びe に対し、F(tG+jY_A , m ×x(eY_A))及びf(tG+jy_A, m ×x(eG))において、３変数t,j,e が２個の代数式で非置換（置き換えられないことを特徴としている。

【００３７】請求項８の発明では、特に特にメッセージ復元型署名の上のrecovery-equation 攻撃を回避するため、写像F_1は、E(GF(p^r))∋G 及びY_A , GF(p^r) ∋m 並びにZ$_q$ = {0,1,…,q-1} ∋t, j及びe に対し、f(tG+jY_A , m ×x(eY_A))及びf(tG+jY_A , m ×x(eG))において、３変数t,j,e が２個の代数式で非置換である（置き換えられない）ことを特徴としている。

【００３８】請求項９の発明では、特に特にメッセージ復元型署名の上のhomomorphism攻撃を回避するため、写像f は、GF(p) ∋r_1, r_2, m, g及びy_A に対し、r_2=f(r_1,m)の逆像をm=f^{-1}(r_1,r_2) で定義するとき、任意の２変数関数φ, ψに対して$f^{-1}(r_1/g, r_2) \neq \phi(m,g)$ 及び$f^{-1}(r_1/y_A, r_2) \neq \psi(m,y_A)$ となることを特徴としている。

【００３９】請求項１０の発明では、特に特にメッセージ復元型署名の上のhomomorphism攻撃を回避するため、写像f_1は、GF(p^r) ∋r_1, r_2, m, g及びy_A に対し、r_2=f_1(r_1,m) の逆像をm=f_1^{-1}(r_1,r_2) で定義するとき、任意の２変数関数φ, ψに対して$f_1^{-1}(r_1/g, r_2) \neq \phi(m,g)$ 及び$f_1^{-1}(r_1/y_A, r_2) \neq \psi(m,y_A)$ となることを特徴としている。

【００４０】請求項１１の発明では、特に特にメッセージ復元型署名の上のhomomorphism攻撃を回避するため、写像F は、E(GF(p))∋R_1, Y_A 及びG 並びにGF(p) ∋ m及びr_2に対し、r_2=f(R_1,m)の逆像をm=f^{-1}(R_1,r_2) で定義するとき、任意の２変数関数φ, ψに対して$f^{-1}(R_1\text{-}G, r_2) \neq \phi(m,G)$ 及び$f^{-1}(R_1\text{-}Y_A, r_2) \neq \psi(m,Y_A)$ となることを特徴としている。

【００４１】請求項１２の発明では、特に特にメッセージ復元型署名の上のhomomorphism攻撃を回避するため、写像F_1は、E(GF(p^r))∋R_1, Y_A 及びG 並びにGF(p^r) ∋ m及びr_2に対し、r_2=f(R_1,m)の逆像をm=f^{-1}(R_1,r_2) で定義するとき、任意の２変数関数φ, ψに対して$f^{-1}(R_1\text{-}G, r_2) \neq \phi(m,G)$ 及び$f^{-1}(R_1\text{-}Y_A, r_2) \neq \psi(m,Y_A)$ となることを特徴としている。

【００４２】請求項１３の発明では、特にメッセージ復

元型署名の上のrecovery-equation,homomorphism攻撃を回避するため、写像f は、(r, y)→r +y(GF(p) 上の加算)で定義されることを特徴としている。請求項１４の発明では、特にメッセージ復元型署名の上のrecovery-equation,homomorphism攻撃を回避するため、写像f1は、(r, y)→r +y(GF(p^r) 上の加算) で定義されることを特徴としている。

【００４３】請求項１５の発明では、特にメッセージ復元型署名の上のrecovery-equation,homomorphism攻撃を回避するため、写像F は、楕円曲線のｘ座標関数を用いて、(R, y)→x(R)+y(GF(p) 上の加算) で定義されることを特徴としている。請求項１６の発明では、特にメッセージ復元型署名の上のrecovery-equation,homomorphism攻撃を回避するため、写像F1は、楕円曲線のｘ座標関数を用いて、(R, y)→x(R)+y(GF(p^r) 上の加算) で定義されることを特徴としている。

【００４４】請求項１７の発明では、特にメッセージ復元型署名の上のrecovery-equation,homomorphism攻撃を回避するため、写像πは、$\{\alpha_1, \alpha_2, \cdots, \alpha_r\}$ をGF(p^r) のGF(p) 上の基底とするとき、GF(pr)の元ｘ＝$x_1\alpha_1 + \cdots + x_r\alpha_r$ ($x_1, \cdots, x_r \in GF(p)$)に対して、$\pi(x) = x_1 + x_2 p + \cdots + x_r p^{r-1}$ で定義されることを特徴としている。

【００４５】請求項１８の発明では、GF(p) 上のメッセージ復元型署名の上の攻撃を回避するため、p を素数とし、有限体GF(p) の元をg とし、その位数をq とし、GF(p)上定義される署名方式において、署名者A の秘密鍵をx_A 、公開鍵を$y_A = g^{x_A}$とし、署名したい文をm ∈GF(p) とするとき、k を署名者が任意にとる乱数とし、r_2をコミットメント$r_1 = g^k$ とm により計算されるGF(p) の元とし、$r_2' \equiv r_2 \pmod q$ とし、ha, hb, hcを有限環$Z_q \times Z_q \times Z_q$ からZ_q への写像とするとき、署名式を、$ha(r_2', s, 1)k \equiv hb(r_2', s, 1) + hc(r_2', s, 1)x_A \pmod q$ からsが計算できるように構成することを特徴としている。

【００４６】請求項１９の発明では、特にGF(p^r) 上のメッセージ復元型署名の上の攻撃を回避するため、p を素数とし、r を正整数とし、有限体GF(p^r) の元をg とし、その位数をq とし、GF(p^r) 上定義される署名方式において、署名者A の秘密鍵をx_A 、公開鍵を$y_A = g^{x_A}$とし、署名したい文をm ∈GF(p^r) とするとき、k を署名者が任意にとる乱数とし、r_2をコミットメント$r_1 = g^k$とm により計算される有限環Z_{p^r}の元とし、$r_2' \equiv r_2 \pmod q$ とし、ha, hb, hcを有限環$Z_q \times Z_q \times Z_q$ からZ_q への写像とするとき、署名式を、$ha(r_2', s, 1)k \equiv hb(r_2', s, 1) + hc(r_2', s, 1)x_A \pmod q$からs が計算できるように構成することを特徴としている。

【００４７】請求項２０の発明では、特にE(GF(p))上のメッセージ復元型署名の上の攻撃を回避するため、p を素数とし、有限体GF(p) 上定義された楕円曲線をE とし、E(GF(p))の元をG とし、その位数をq とし、E(GF(p))上定義される署名方式において、署名したい文をm ∈GF(p) とするとき、k を署名者が任意にとる乱数とし、r_2をコミットメント$R_1 = kG$ とm により計算されるGF(p) の元とし、$r_2' \equiv r_2 \pmod q$ とし、ha, hb, hcを有限環$Z_q \times Z_q \times Z_q$ からZ_q への写像とするとき、署名式を、$ha(r_2', s, 1)k \equiv hb(r_2', s, 1) + hc(r_2', s, 1)x_A \pmod q$ からsが計算できるように構成することを特徴としている。

【００４８】請求項２１の発明では、特にE(GF(p^r) 上のメッセージ復元型署名の上の攻撃を回避するため、p を素数とし、r を正整数とし、有限体GF(p^r) 上定義された楕円曲線をE とし、E(GF(p^r))の元をG とし、その位数をq とし、E(GF(p^r))上定義される署名方式において、署名したい文をm ∈GF(pr)とするとき、k を署名者が任意にとる乱数とし、r_2をコミットメント$R_1 = kG$ とmにより計算される有限環Z_{p^r}の元とし、$r_2' \equiv r_2 \pmod q$ とし、ha, hb, hcを有限環$Z_q \times Z_q \times Z_q$ からZ_q への写像とするとき、署名式を、$ha(r_2', s, 1)k \equiv hb(r_2', s, 1) + hc(r_2', s, 1)x_A \pmod q$ からs が計算できるように構成することを特徴としている。

【００４９】請求項２２の発明では、特にメッセージ復元型署名の上のsignature-euqaion攻撃を回避するため、写像ha,hb, hc は、r_2',s をZ$_q$ の元とするとき、予め固定された少数値を除く任意のZ$_q$ の元rr_2', ssに対して、次の二つの条件1. $ha(r_2', s, 1) = ha(rr_2', ss, 1)$, $hc(r_2', s, 1) = hc(rr_2', ss, 1)$ のとき$hb(r_2', s, 1) - ha(r_2', s, 1) \neq hb(rr_2', ss, 1)$2. $ha(r_2', s, 1) = ha(rr_2', ss, 1)$, $hb(r_2', s, 1) = hb(rr_2', ss, 1)$のとき$hc(r_2', s, 1) - ha(r_2', s, 1) \neq hc(rr_2', ss, 1)$ を満足することを特徴としている。

【００５０】請求項２３の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像ha,hb,hcは、$ha(r_2', s, 1) = r_2'$, $hc(r_2', s, 1) = s$とし、$hb(r_2', s, 1)$ は、$r_2' = rr_2'$, s=ssのとき、$hb(r_2', s, 1) = hb(rr_2', ss, 1)$ 、$r_2' = rr_2'$, $hb(r_2', s, 1) = hb(rr_2', ss, 1)$ のとき、s=ss、hb(0, 0, 1) ≠0,を満たすことを特徴としている。

【００５１】請求項２４の発明では、特にメッセージ復元型署名の上のsignature-equation, 比例攻撃を回避するため、写像ha,hb,hcは、$ha(r_2', s, 1) = s$, $hc(r_2', s, 1) = r_2'$とし、$hb(r_2', s, 1)$ は、s=ss, $r_2' = rr_2'$, のとき、$hb(r_2', s, 1) = hb(rr_2', ss, 1)$、s=ss, $hb(r_2', s, 1) = hb(rr_2', ss, 1)$ のとき、$r_2' = rr_2'$、hb(0, 0, 1) ≠0 を満たすことを特徴としている。

【００５２】請求項２５の発明では、特にメッセージ復元型署名の上のsignature-equation, 比例攻撃を回避するため、写像ha,hb,hcは、$ha(r_2', s, 1) = s$, $hb(r_2', s, 1) = r_2'$とし、$hc(r_2', s, 1)$ は、$r_2' = rr_2'$, s=ssのとき、$hc(r_2', s, 1) = hc(rr_2', ss, 1)$ 、s=ss, $hc(r_2', s, 1) = hc(r$

r_2',ss,1) のとき、r_2'=rr_2'hc(0, 0, 1) ≠0 を満たすことを特徴としている。

【００５３】請求項２６の発明では、特にメッセージ復元型署名の上のsignature-equation, 比例攻撃を回避するため、写像ha,hb,hcは、ha(r_2',s,1)=r_2', hb(r_2',s,1)=sとし、hc(r_2',s,1) は、r_2'=rr_2', s=ssのとき、hc(r_2',s,1)=hc(rr_2',ss,1) 、r_2'=rr_2', hc(r_2',s,1)=hc(rr_2',ss,1) のとき、s=ss、hc(0, 0, 1) ≠0 を満たすことを特徴としている。

【００５４】請求項２７の発明では、特にメッセージ復元型署名の上のsignature-equation, 比例攻撃を回避するため、写像ha,hb,hcは、hc(r_2',s,1)=s, hb(r_2',s,1)=r_2'とし、ha(r_2',s,1) は、r_2'=rr_2', ha(r_2',s,1)=ha(rr_2',ss,1) のとき、s=ss、s=ss, ha(r_2',s,1)=ha(rr_2',ss,1) のとき、r_2'=rr_2'、ha(0,0,1) ≠0 を満たすことを特徴としている。

【００５５】請求項２８の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像ha,hb,hcは、hc(r_2',s,1)=r_2', hb(r_2',s,1)=sとし、ha(r_2',s,1) は、r_2'=rr_2', ha(r_2',s,1)=ha(rr_2',ss,1) のとき、s=ss、s=ss, ha(r_2',s,1)=ha(rr_2',ss,1)のとき、r_2'=rr_2'、ha(0,0,1) ≠0 を満たすことを特徴としている。

【００５６】請求項２９の発明では、特にメッセージ復元型署名のsignature-equation、比例攻撃を回避するため、写像hb(r_2',s,1) は、hb(r_2',s,1)=r_2' ＋s ＋1 で定義されることを特徴としている。請求項３０の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像hb(r_2',s,1) は、hb(r_2',s,1)=r_2' ×s ＋1 で定義されることを特徴としている。

【００５７】請求項３１の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像hc(r_2',s,1) は、hc(r_2',s,1)=r_2' ＋s ＋1 で定義されることを特徴としている。請求項３２の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像hc(r_2',s,1) は、hc(r_2',s,1)=r_2' ×s ＋1 で定義されることを特徴としている。

【００５８】請求項３３の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像ha(r_2',s,1) は、ha(r_2',s,1)=0 となる解(r_2',s) が有限時間（ビットデータの多項式、すなわち非指数時間）で確定できることを特徴としている。請求項３４の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、乱数k を、メッセージマスク式で計算されるr_2と署名式で計算されるs に対して、ha(r_2',s,1) ≠0 であるように取ってくることを特徴としている。

【００５９】請求項３５の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像ha(r_2',s,1) は、ha(r_2',s,1)=r_2'+s+1 であることを特徴としている。請求項３６の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像ha(r_2',s,1) は、ha(r_2',s,1)=r_2' ×s ＋1 であることを特徴としている。

【００６０】請求項３７の発明では、特にGF(p) 上のメッセージ復元型署名の上の攻撃を回避するため、p を素数とし、q を（Ｐ／４）＜qとなる正整数とし、有限体GF(p) の位数がq となる元をg とし、GF(p) 上定義される署名方式において、署名したい文をm ∈GF(p) とするとき、乱数k を、コミットメントr_1＝g ^{k} とm により構成されるGF(p) の元r_2が、０＜r_2＜q となるようにとり、上記範囲を限定されたr_2を署名式に用いることを特徴としている。

【００６１】請求項３８の発明では、特にGF(p^r) 上のメッセージ復元型署名の上の攻撃を回避するため、 pを素数とし、r を正整数とし、q を（Ｐ／４）＜qとなる正整数とし、有限体GF(p^r) の位数がq となる元をg とし、GF(p^r) 上定義される署名方式において、署名したい文をm ∈GF(p^r) とするとき、乱数k を、コミットメントr_1＝g ^{k} とm により構成されるZ_{p^r}= {0,1,…,p^{r-1} } の元r_2が、０＜r_2＜q となるようにとり、上記範囲を限定されたr_2を署名式に用いることを特徴としている。

【００６２】請求項３９の発明では、特にE(GF(p))上のメッセージ復元型署名の上の攻撃を回避するため、p を素数とし、有限体GF(p) 上定義された楕円曲線をE とし、E(GF(p))の元をG とし、その位数をq とし、E(GF(p))上定義される署名方式において、署名したい文をm ∈GF(p) とするとき、乱数k を、コミットメントr_1＝g ^{k}とm により構成されるGF(p) の元r_2が、０＜r_2＜q となるようにとり、上記範囲を限定されたr_2を署名式に用いることを特徴としている。

【００６３】請求項４０の発明では、特にGF(p^r) 上のメッセージ復元型署名の上の攻撃を回避するため、p を素数とし、r を正整数とし、有限体GF(p^r) 上定義された楕円曲線をE とし、E(GF(p^r))の元をG とし、その位数をq とし、E(GF(p^r))上定義される署名方式において、署名したい文をm ∈GF(p^r) とするとき、乱数k を、コミットメントr_1＝g ^{k} とm により構成されるZ_{p^r}= {0,1,…,p^{r-1} } の元r_2が、０＜r_2＜q となるようにとり、上記範囲を限定されたr_2を署名式に用いることを特徴としている。

【００６４】請求項４１の発明では、特にE(GF(p))上のメッセージ復元型署名の上の攻撃を回避するため、楕円曲線E は、元の個数がp となるGF(p) 上の楕円曲線を用いることを特徴としている。請求項４２の発明では、特にメッセージ復元型署名の上の攻撃を回避するため、署名したい文m に対し、m のハッシュ関数値hash(m) をm

の代わりに用いることを特徴としている。請求項４３の発明では、特にE(GF(p))上のメッセージ復元型署名の上の攻撃を回避するため、p を素数とし、有限体GF(p) の元をg とし、その位数をq とし、GF(p) 上定義される署名方式において、署名者A の秘密鍵をx_A、公開鍵を$y_A=g^{x_A}$とし、署名したい文をm ∈GF(p) とするとき、k を署名者が任意にとる乱数とし、コミットメント$r_1=g^k$とし、$r_1' \equiv r_1 \pmod q$, $m' \equiv m \pmod q$とし、ha, hb, hcを有限環$Z_q \times Z_q \times Z_q$から$Z_q$への写像とするとき、署名式を、$ha(r_1',s,m')k \equiv hb(r_1',s,m') + hc(r_1',s,m')x_A \pmod q$からs が計算できるように構成することを特徴としている。

【００６５】請求項４４の発明では、特にE(GF(p))上のメッセージ復元型署名の上の攻撃を回避するため、p を素数とし、r を正整数とし、有限体GF(p^r) の元をg とし、その位数をq とし、GF(p^r) 上定義される署名方式において、署名者A の秘密鍵をx_A、公開鍵を$y_A=g^{x_A}$とし、署名したい文をm ∈GF(p^r) とするとき、k を署名者が任意にとる乱数とし、コミットメント$r_1=g^k$とし、GF(p^r) から有限環Z_{p^r}への写像をπとするとき、$r_1' \equiv \pi(r_1) \pmod q$, $m' \equiv \pi(m) \pmod q$とし、ha, hb, hcを有限環$Z_q \times Z_q \times Z_q$から$Z_q$への写像とするとき、署名式を、$ha(r_1',s,m')k \equiv hb(r_1',s,m') + hc(r_1',s,m')x_A \pmod q$からs が計算できるように構成することを特徴としている。

【００６６】請求項４５では、特にE(GF(p))上のメッセージ復元型署名の上の攻撃を回避するため、p を素数とし、有限体GF(p) 上定義された楕円曲線をE とし、E(GF(p))の元をG とし、その位数をq とし、E(GF(p))上定義される署名方式において、署名したい文をm ∈GF(p) とするとき、k を署名者が任意にとる乱数とし、コミットメント$R_1=kG$とし、E(GF(p))からGF(p) への写像をρとするとき、$r1' \equiv \rho(R_1) \pmod q$, $m' \equiv m \pmod q$とし、ha, hb, hcを有限環$Z_q \times Z_q \times Z_q$から$Z_q$への写像とするとき、署名式を、$ha(r_1',s,m')k \equiv hb(r_1',s,m') + hc(r_1',s,m')x_A \pmod q$からs が計算できるように構成することを特徴としている。

【００６７】請求項４６の発明では、特にE(GF(p))上のメッセージ復元型署名の上の攻撃を回避するため、p を素数とし、r を正整数とし、有限体GF(p^r) 上定義された楕円曲線をE とし、E(GF(p^r))の元をG とし、その位数をq とし、E(GF(p^r))上定義される署名方式において、署名したい文をm ∈GF(p^r) とするとき、k を署名者が任意にとる乱数とし、コミットメント$R_1=kG$とし、E(GF(p^r))からGF(p^r)への写像をρとするとし、GF(p^r) から有限環$Z_{p^r}=\{0,1,\cdots,p^{r-1}\}$への写像をπとするとき、$r_1' \equiv \pi(\rho(R_1)) \pmod q$, $m' \equiv \pi(m) \pmod q$とし、ha, hb, hcを有限環$Z_q \times Z_q \times Z_q$から$Z_q$への写像とするとき、署名式を、$ha(r_1',s,m')k \equiv hb(r_1',s,m') + hc(r_1',s,m')x_A \pmod q$からs が計算できるように構成することを特徴としている。

【００６８】請求項４７の発明では、特にE(GF(p))上のメッセージ復元型署名の上の攻撃を回避するため、写像ρは、楕円曲線のｘ座標若しくはｙ座標関数を用いて、R →x(R)若しくはR→ｙ（Ｒ）で定義されることを特徴としている。請求項４８の発明では、特にE(GF(p))上のメッセージ復元型署名の上の攻撃を回避するため、写像πは、$\{\alpha_1, \alpha_2, \cdots, \alpha_r\}$をGF($p^r$) のGF(p) 上の基底とするとき、GF($p^r$) の元$x=x_1\alpha_1 + \cdots + x_r\alpha_r$（$x_1, \cdots, x_r \in$GF(p))に対して、$\pi(x)=x_1+x_2p+\cdots+x_r p^{r-1}$で定義されることを特徴としている。

【００６９】

【実施例】

（第１実施例）以下、本発明を実施例に基づいて説明する。以下、本発明の第１実施例を、図を参照しつつ説明する。まず、公開ディジタル通信網全体の構成について説明する。

【００７０】図６は、本発明が実施される公開ディジタル通信網全体の構成図である。本図において、１は通信網提供者である。２は、公開ディジタル通信回線である。２はディジタル通信回線である。３～６は、公開ディジタル通信回線２に接続されたユーザ端末（以下、単に「ユーザ」と言う）Ａ、ユーザＢ、…、ユーザＵ、ユーザＶである。本図に示すように、通信網提供者は、システムパラメータとして、２進数５１２ビットで表される素数ｐ、

$g^q \equiv 1 \pmod p$

となる最小の整数（位数）ｑが２５６ビットの整数ｑである整数ｇ、ＧＦ（ｐ）上でｆ（r_1, ｍ）≡r_1 ＋ｍ（ｍｏｄ ｐ）そしてその逆字像f^{-1}がf^{-1}（r_1，ｆ（r_1，ｍ））≡ｍ （ｍｏｄ ｐ）を充たすメッセージマスク式ｆ，Ｚｇ×Ｚｇ×ＺｇからＺｇへの写像で、ｈａ（r_2'，ｓ，１）＝ｓ、ｈｂ（r_2'，ｓ，１）≡r_2'＋ｓ＋１（ｍｏｄ ｑ）、ｈｃ（r_2'，ｓ，１）r_2'を充たす関数ｈａ、ｈｂ、ｈｃをシステムパラメータと各ユーザに公開している。

【００７１】次に、図６に示す通信網提供者１とユーザ３～６の構成について説明する。図７は、通信網提供者１により提供されたＩＣカードやユーザ自身が作成したパソコン用プログラムの要部の構成図である。本図において、１１は秘密鍵作成要求受付部である。１２は、秘密鍵発生部である。１３は、公開鍵作成部である。１４は、公開鍵公開部である。１５は、秘密鍵通知形態作成部である。１６は、秘密鍵通知部である。

【００７２】１３１は公開鍵作成部１３内のｇの2^nのｐを法とする剰余記憶部である。１３２は、同じく法取り出し部である。１３３は、同じく乗算部である。１３４は、同じく割算部である。以下、上記各部の作用等について説明する。秘密鍵作成要求受付部１１は、各ユー

ザ３～６（本図ではユーザＡ）からの固有の秘密鍵の作成要求を、ユーザのキーボードを使用しての操作等で受け付ける。秘密鍵発生部１２は、秘密鍵作成要求受付部１１が受け付けた要求をもとに、内蔵する乱数発生プログラムにより２進数の乱数を発生させ、これを当該ユーザの秘密鍵とする。なお、本実施例では、乱数の発生に際しては、同一の乱数発生を万が一にも防止し、併せて整理の都合もあるため当該ユーザの公開ディジタル通信網上での識別番号をも組み込んだものとしている。またこのため、乱数はｐと同じく５１２ビットとしている。公開鍵作成部１３は、２進乱数発生部１２の発生させた乱数をもとに公開鍵を作成する。なお、この手順は、後で詳しく説明する。

【００７３】公開鍵公開部１４は、公開鍵作成部１３の作成した公開鍵をその作成要求をなしたユーザ名と共に、全ユーザに公開する。これは、通信網が正当性を承認したユーザ名との公開鍵を対応して登録し、ＲＯＭ等で発行し、また各ユーザの問い合わせに回答する。秘密鍵通知形態作成部１５は、各ユーザの秘密鍵をその操作ミスで外部へ漏出しないよう保護する。秘密鍵通知部１６は、秘密鍵を共有鍵の作成等の必要に応じて使用しうるようにする。

【００７４】次に、公開鍵作成部１３による公開鍵の作成について説明する。公開鍵作成部１３は、ｇの2^n乗のｐを法とする剰余記憶部１３１と法取り出し部１３２と、乗算部１３０と割算部１３４とを有する。ｇの2^nのｎを法とする剰余記憶部１３１は、ｇ、g^2、g^4、g^8…等ｇの２の累べき剰のｐを法とする剰余g_1、g_2…、g_iをあらかじめ計算して、ＲＯＭに記憶している。これを小さい数を例にとって、具体的に示す。ｐ＝１１、ｇ＝2ならば、ｉ＝〔$\log_2$　１１〕＝３となり、2^3＜１１となるため、ｇ、g^2、g^4として２、2^2、2^4を、更に対応するg_1、g_2、g_4として２、４、５を記憶している。法取り出し部１３２は、秘密鍵発生部１２から２進数で表現された秘密鍵の通知を受けると、その値で１が立つ桁に対応するg_1、g_2、…、g_iを取り出す。これも、小さい数を例にとって具体的にする。今ｘａ＝１０１（１０進の５）とする。１位と３位（各、ｇの２の０乗と２の２乗）に１が立っている。このためg_1とg_4、すなわち２と５を取り出す。乗算部１３３は、法取り出し部１３２の取り出した法を掛け合わせる。割算部１３４は、乗算部１３３の乗算結果をｎで割り、その剰余を求める。上記具体的数値で示すならば、$2^{xa}=2^5=2\times2^4=2\times5=10$（mod 11）となる。そして、この剰余がユーザAの公開鍵とされる。なお、本実施例でｇの累べきを剰を採用しているのは、g^3、g^5等の法を採用するのよりも一般的に処理が速く、演算機等も２進で作動することにあわせたものである。

【００７５】次に、署名付きの送信を行うユーザＡ側の重要な処理の流れを図８に、重要な構成を図９と図１０に示す。図９において、３１はr_2制御部である。３２は２進乱数発生部である。３３はr_1演算部である。３４は、通信文（ｍ）入力部である。３５は、ｆ関数部である。３６は、ｑ記憶部である。３７は、排除部である。また、３３１は、r_1演算部内のべき剰余記憶部である。また、３３２は、同じく法取り出し部である。３３３は、同じく乗算部である。３３４は、同じく割算部である。３５１は、ｆ関数部３５内の和算部である。３５２は、同じく、割算部である。３７１は、排除部３７内のｑ読み出し出力部３７１である。３７２は、同じく引き算部である。３７３は、同じく比較部である。

【００７６】図１０において、３８はＳＫ部である。３８１は、ＳＫ部３８内のｋ－１演算部である。３８２は、同じくr_2+1演算部である。３８３は、同じく$r_2\ x_A$演算部である。３８４は、同じく$r_2+1+r_2\ x_A$演算部である。３８５は、同じく、Ｓ計算部である。以下、上記各部の作用等について説明する。

【００７７】最初、システムパラメータの入手（ａ１）と秘密鍵等の作成操作（ａ２）がなされ、秘密鍵の作成及び公開鍵の登録がなされる（ａ３）。r_2制御部３１は、署名通信発信にあたり、２進乱数発生部３２とｍ入力部３４の作用を調整、制御し、後に説明するが、必要な繰り返し処理をも行う。通信文入力部３４は、署名発信のための文、例えば「私は、特発　許明です。電話番号は０３―３５８１―１１０１。確認願います。」等の文書をユーザにより入力され、これを数値（ｍ）化する（ａ４）。

【００７８】２進乱数発生部３２は、コミットメント作成のため署名発信毎に相異なる乱数を発生をさせる。またこのため、発信日時等も乱数発生に使用される。（ａ５）

r_1演算部３３は、発生された２進乱数ｋをもとに$r_1\equiv g^k$（mod　ｐ）の演算により、r_1を求める。このため、通信網提供者におけるｇの2^nのｐを法とする剰余記憶部１３１、法取り出し部１３２、乗算部１３３、割算部１３４と同じ構成作用をなす剰余記憶部３３１、法取り出し部３３２、乗算部３３３、割算部３３４を有している。（ａ６）

ｆ関数部３５は、r_1演算部３３で作成されたr_1と通信文入力部３４で数値化された通信文ｍをもとに、メッセージマスク式ｆを使用して、$r_2\equiv f(r_1, m)$（mod ｐ）の演算を行い、r_2を求める。（ａ７）

このため、（mod ｐ）上での$r_2\equiv r_1+m$の和算を行う和算部３５１と、和のｐを法とする剰余を求めるためｐでの割算を行う割算部３５２とを内蔵している。

【００７９】ｑ記憶部３６は、あらかじめ別途ユーザにより入力されたｇをメモリーに記憶している。排除部３７は、ｆ関数部３５から入力されたr_2とｑとの大小比較を行い（ａ８）、r_2がｑ以上となれば、前述の冗長

攻撃を回避すべくこの送信を行わず、この旨r_2制御部３１に通知する。

【００８０】この通知を受けた、r_2制御部３１は、２進乱数発生部３２に再度異なる乱数発生をなさしめて（ａ９）先のr_1と異なるr_1を得、これと通信文入力部３４に入力されている通信文ｍとでｆ関数を部３５にｆ関数作用させｔｅ、先と異なるr_2を求め、更にｑとの大小比較を行わしめるというプロセスを、$g-r_2$が正となるまで繰り返し実行させる。また、$q-r_2$が正となれば、このr_2をＳＫ部３７へ出力する。またこのため、排除部３７は、ｑ読み出し部３７１と引き算部３７２と比較部３７３とを内蔵している。ｑ読み出し部３７１は、r_2の入力があるとｑ記憶部３６からｑの値を読み出し、引き算部３７２に通知する。引き算部３７２は、通知されたｑからr_2の引き算を行う。比較部３７３は、引き算部３７２の求めた差が０より小ならばr_2制御部３１へこの旨通知するこのため、この値が正となるまで上述の手順を繰り返し実行されることとなる。また、r_2が正ならば、入力されたr_2をそのままＳＫ部へ通知する。

【００８１】ＳＫ部３８は、署名式ｓＫ≡（r_2＋ｓ＋１）＋r_2 x_a（ｍｏｄ ｐ）の演算により、送信対象となるメッセージを作成する（ａ１０）。図１４に示すような構成である。そして、内蔵しているｋ－１演算部３８１は、２進乱数発生部３８１にて発生された、そしてそれを使用して計算したr_2の値ががｑ未満という要件を充たすこととなった乱数ｋから１を引き去る。なお、この差をａとする。

【００８２】同じく、r_2＋１演算部３７は、入力されたr_2に１を加える。同じく、r_2 x_a演算部３８３は、排除部３７から入力されたr_2と図示しない秘密鍵記憶部から入力されたx_Aとの積を求める。r_2＋１＋r_2 x_A演算部３８４は、r_2＋１演算部３８２から入力されたr_2＋１とr_2 x_A演算部３８３から入力されたr_2 x_Aとの和を求める。なお、この和をｂとする。ｓ計算部３８５は、ｋ－１演算部３８１が求めたａとr_2＋１＋r_2 x_A演算部３８４が求めたｂとを使用して、ｓ・ａ≡ｂ（ｍｏｄ ｑ）を充たすｓをユークソッドの互除法により求める。そしてこの結果を図示しない送信部へ送る。

【００８３】以上のもとで、署名を求める他のユーザＢへ、（r_2，ｓ）が署名文として送信されることとなる。（ａ１１）

図１１は、署名文を受信したユーザ側の重要な処理の流れを示す図であり、図１２は構成図である。本図において、４１は受信部である。４２は、拒絶部である。４３は、ｑ記憶部である。４４は、ｙａ記憶部である。４５は、r_2記憶部である。４６は、ｓ記憶部である。４７は、ｇ記憶部である。４８は、r_2＋ｓ＋１演算部である。４９は、$y_A^{1/S}$（ｍｏｄ ｐ)演算部である。４１０は、g^S（ｍｏｄ ｐ)演算部である。４１１は、$y_A^{r2/s}$（ｍｏｄ ｐ)演算部である。４１２は、$g^{(r2+1+S)/S}$（ｍｏｄ ｐ)演算部である。４１３は、$r_1 \equiv g^{(r2+1+S)/S} y_A^{r2/S}$（ｍｏｄ Ｐ)演算部である。４１４は、$f^{-1}$関数部である。

【００８４】受信部４１は、認署を求める他のユーザ、今Ａとする、からの送信文（r_2，Ｓ）を受信する（ｂ１）。拒絶部４２は、受信があった場合、r_2－ｑを計算し（ｂ２）、正なら一応正当なものとして続行する処理を行うべく他部にこの受信文を流すが、正でなければこの署名を拒否する（ｂ３）。またこのため、送信側ユーザと同じくｑ記憶部４３にあらかじめｑを記憶している。y_A記憶部４４は、通信網提供者より公開されたy_Aを、あらかじめメモリーに記憶している。

【００８５】ｇ記憶部４７も、同じくあらかじめｇを記憶している。r_2記憶部４５は、拒絶部４２が一応認署したr_2を記憶し、ｓ記憶部４６は同じくｓを記憶する。なお、r_2とｓの区分けは、別途定めた通信規約に基づきなされる。r_2＋ｓ＋１演算部４８は、r_2記憶部４５とｓ記憶部４６からそれぞれr_2とｓを読み出し、和算でr_2＋ｓ＋１を求める。$y_A^{1/S}$（ｍｏｄ ｐ)演算部４９は、y_A記憶部４４からy_Aを：Ｓ記憶部４６からｓを読み出して$y_A^{1/S}$（ｍｏｄ ｐ)を演算する。g^S（ｍｏｄ ｐ)演算部４１０は、ｓ記憶部４６からｓを、ｇ記憶部４７からｇを読み出して、$g^{1/S}$（ｍｏｄ ｐ)を演算する。$y_A^{r2/S}$（ｍｏｄｐ)演算部４１１は、r_2記憶部４５から読み出したr_2と$y_A^{1/S}$（ｍｏｄ ｐ)を演算部４９から読み出した$y_A^{1/S}$（ｍｏｄ ｐ)をもとに），（$y_A^{1/S}$）をr_2乗し、更にそのｐを法とする剰余を求める。$g^{(r2+1+S)/S}$（ｍｏｄ ｐ)演算部４１２は、r_2＋ｓ＋１演算部４１８からr_2＋ｓ＋１を読み出し、$g^{1/S}$（ｍｏｄ ｐ)演算部４１０から読み出した$g^{1/S}$（ｍｏｄ ｐ)をr_2＋ｓ＋１乗し、更にこのｐを法とする剰余を求める。

【００８６】$r_1 \equiv g^{(r2+1+S)/S} y_A^{r2/S}$（ｍｏｄ ｐ)演算部４１３は、$y_A^{r2/S}$（ｍｏｄ ｐ)演算部４１１の演算結果と$g^{(r2+1+S)/S}$（ｍｏｄ ｐ)演算部４１２の演算結果とから、$r_1 \equiv g^{(r2+1+S)/S} y_A^{r2/S}$（ｍｏｄ ｐ)の演算により、$r_1$を求める（ｂ４）。$f_1$関数部４１４は、関数$f^{-1}$を使用して演算$r_2$－$r_1$を行い、ｍを求める（ｂ５）。

【００８７】以上の構成により、ユーザＢはユーザＡの送信文からｍを入手するが、この際通信網提供者が公開したy_Aに相当する秘密鍵x_aを知っているのはユーザＡのみであり、またこのx_aを使用しない限りy_aを使用しての正しい復号もなしえばい。このため、送信者は、確かにユーザＡの署名であると確認する（ｂ６）。次に、以上の説明とかなり重複するが、以上の手順における通信文の処理、各種の数式をもとにしての、式や数値で表現されたデータの変化の様子を中心として、この

手順を説明する。

【００８８】図１は、この数値式や面で表現した手順の基本的な構成を示すものである。以下、本図を参照しながら実施例の手順を説明する。

（１）センターによる初期設定

p を素数とし、GF(p) の元をg としその位数をq とする。ここでp ～q ととる。

【００８９】GF(p) ×GF(p) からGF(p) への写像f を、

$f(r_1, m) \equiv r_1 + m \pmod{p}$

f の逆写像f を

$f^{-1}(r_1, f(r_1, m)) \equiv m \pmod{p}$

とし、Zq×Zq×ZqからZqへの写像 h_a ,h_b ,h_c を、$ha(r_2', s, 1)=s$, $hc(r_2', s, 1)=r_2'$とし、

$hb(r_2', s, 1) \equiv r_2' + s + 1 \pmod{q}$

で定義する。また署名式を

$ha(r_2', s, 1)k \equiv hb(r_2', s, 1) + hc(r_2', s, 1)x_A \pmod{q}$

で定義する。

【００９０】センターは、システムパラメータとしてp ，q ，g ，f，ha，hb，hc を公開する。この状態が、図６に示すものである。

（２）ユーザによる署名送信のための秘密鍵の作成及びセンターが認署した公開鍵の登録。

【００９１】ユーザＡが、メッセージ復元型署名通信を行うため、その秘密鍵を基に公開鍵を作成し、これを通信網提供者が正しいものとして登録する要求を行う。この要求のため、ユーザＡはその端末識別番号を使用して乱数を発生させ、秘密鍵X_Aを生成する。次いで、その公開値$y_A \equiv g^{X_A} \pmod{p}$を生成し、生成した公開値はセンターを通じて各ユーザに通知される。

（３）ユーザＡによる署名の生成及び送付

１．２進乱数k を、プログラムにのっとって生成する。

【００９２】２．以下の演算を順に行う。

2-1)$r_1 \equiv g^k \pmod{p}$ ，

2-2)$r_2 \equiv f(r_1, m) \pmod{p}$ …(c) とする。

2-3) $q \leq r_2$の場合、再度上記１に戻り、異なる２進乱数を生成する。

2-4)$sk \equiv (r_2+s+1)+r_2x_a \pmod{q}$…(d) よりs を計算する。

【００９３】３．上記２で生成した(r_2 ，s)をユーザＢに送信する。

（４）ユーザＢによる受信したメッセージの復元

1. q ≦r_2ならば、署名を拒絶する。

2. $r_1 \equiv g^{(r2+s+1)/s} y_A^{r2/s} \pmod{p}$を計算し、

$f^{-1}(r_1, r_2) \equiv m \pmod{p}$

を計算することにより、メッセージm を復元する。

【００９４】次に、以上の署名の耐攻撃性について説明する。以上の構成のメッセージ復元型署名の場合、コミットメントr_1が従来例の式(a) のように直接平文m に関与するのでなく、写像f を通して関与している。この写像f が

(*)1: GF(p)∋g, y_A 及びm 並びにZq= {0,1,…,q-1}∋t, j及びe に対し、$f(g^t y_A^j, m y_A^e)$ 及び$f(g^t y_A^j, mg^e)$ において、３変数t,j,e が２個の代数式で非置換である。このため、recovery equation 攻撃を受けない。

【００９５】2: GF(p)∋r_1, r_2, m, g及びy_A に対し、$r_2=f(r_1, m)$の逆像をm=$f^{-1}(r_1, r_2)$ で定義するとき、任意の２変数関数ϕ, ψに対して$f^{-1}(r_1/g, r_2) \neq \phi(m, g)$ 及び$f^{-1}(r_1/y_A, r_2) \neq \psi(m, y_A)$ となることから、宮地らにより提案された３つの攻撃(recovery-equation attack , using g and y_A , and homomorphism attack)を回避できる。

【００９６】また上記実施例のように構成されたメッセージ復元型署名の場合、従来例の式(b')のように署名式の係数(a,b,c) が(r_2',s,1) の置換という形ではなく、写像ha，hb，hcを用いて決定されている。この写像ha，hb，hcが(**)r_2',s をZqの元とするとき、予め固定された少数値をのぞく全てのrr_2', ssに対して、次の二つの条件

1. $ha(r_2', s, 1)=ha(rr_2', ss, 1)$, $hc(r_2', s, 1)=hc(rr_2', ss, 1)$ のとき$hb(r_2', s, 1)-ha(r_2', s, 1) \neq hb(rr_2', ss, 1)$

2. $ha(r_2', s, 1)=ha(rr_2', ss, 1)$, $hb(r_2', s, 1)=hb(rr_2', ss, 1)$のとき$hc(r_2', s, 1)-ha(r_2', s, 1) \neq hc(rr_2', ss, 1)$

を満たすことから、宮地らにより提案された２つの解読(signature-equation attack using g and y_A) を回避できる。さらにこの署名式は従来から存在する比例関係を用いた解読に対しても、署名式が２項に分解されることがないので強い。

【００９７】なお、従来から存在する比例関係を用いた比例攻撃に付いては、L.Harn and Y. Xu, "Design of generalised ElGamal type digital signatureschemes based on discrete logarithm", Electron. Lett., Vol. 30(1994),2025-2026.に詳しい。また、上記実施例のようにp ～q ととることにより、r_2の値を制限するステップ（署名生成ではステップ2-3,メッセージ復元ではステップ１）を付加することができる。これにより宮地により提案された１つの解読(redundancy attack) を回避できる。更にこの場合、qのｐに対する比が従来のごとく2^{-400}と小さくなく、１／３、１／２することにより、再度乱数を発生させ繰り返しての処理を行わねばならない確率も低下しえる。

【００９８】なお、上述の実施例はf をr$_1$＋m として行ったが、これは勿論他の写像f で、(*) を満たすものなら何でもよい。またこの際、r$_1$＋m のように計算量が小さい写像にすることが望ましい。ha，hb，hcに関しても、上記の性質(**)をもつものなら何でもよい。またこの際、従来から存在する比例関係を用いた解読に対しても強くなるように、さらに計算量が小さい写像にすることが望ましい。

【００９９】また、上記の従来例以外のどんなメッセージ復元型署名にも上記の写像を付加すると同様に解読が回避できる。また、上記の署名方式は、メッセージｍに署名する代わりに、ｍにＩＳＯで定められたＲＣ　４、ＲＣ　２等のハッシュ関数を施したハッシュ値に対して署名し、署名をメッセージとともに送り、ハッシュ値が正しく復元されることをチェックすることで署名を確認するという署名方式としても用いることができる。

【００１００】また、上記署名方式は、各ユーザの秘密鍵等は、通信網提供者又はユーザ用の情報発行センターが生成するものとしたが、これは勿論各ユーザが任意にその秘密鍵を選定し、公開値等のみセンターへ登録するようにしてもよい。更に、通信網提供者とユーザ用の情報発行センターが異なってもよい。また、上記署名方式では、各種演算はＧＦ（ｐ）上でなされるものとしたが、これは勿論ＧＦ（p^r）上でなされてもよい、この場合には、上記実施例における（ｍｏｄ ｐ）での演算は（ｍｏｄ p^r）での演算となり、このため、r_1 とｍをＧＦ（p^r）×ＧＦ（p^r）からＧＦ（p^r）へ字像 f_1 を用いて変換した後、この値を更にＧＦ（p^r）から有限環Ｚ p^r ＝｛０，１，…，p^{r-1}｝への変更をなす等の手順が付加される。

【００１０１】なお、この写像πは、｛α_1，α_2，…，α_r｝をＧＦ（p^r）のＧＦ（ｐ）上の基底とするとき、ＧＦ（p^r）の元ｘ＝x_1 α_1 ＋…＋x_r α_r（x_1，x_2，…，x_r ∈ＧＦ（ｐ））に対してπ（ｘ）＝x_1 ＋x_2 ｐ＋…＋x_r p^{r-1}で定義される。この手順を図１３に示す。（注、上記実施例はｒ＝１の場合であり、πは恒等写像となり、表面上でてこない。）

（第２実施例）本実施例は、本発明に係るメッセージ復元型署名方式として、楕円曲線上での演算を行うものである。

【００１０２】本実施例も、基本的な構成、原理は先の第１実施例と異ならない。ただし、有限体ＧＦ（ｐ）上の離散対数問題の困難性でなく、楕円曲線Ｅ（ＧＦ（ｐ））上の困難性を利用するため、これに関係する点が異なる。このため、この相違する点を中心に説明する。ディジタル公開通信網におる通信網提供者１、各ユーザ３～６の接続状態及び初期設定としてのシステムパラメータの概略の構成を図１４に示す。

【００１０３】システムパラメータとしてＥ（ＧＦ（ｐ））と、ｇに換えてのＥ（ＧＦ（ｐ））上の零元と異なる元Ｇが加えられ、ｐは１０進３０桁の素数である。これは、Ｅ（ＧＦ（ｐ））上の離散対数問題は有限体上でのそれに比較してはるかに困難であることによる。ｑがないが、これは、Ｇのの位数は零元を除き常にｐであることによる。また、楕円曲線を使用するため、ｆはｘ座標関数である。

【００１０４】各部の構成であるが、第１実施例では、ｐを法とする g^k の剰余を計算するため通信網提供者１及びユーザ側の剰余記憶部１３１、２３１等には、ｇ，g^2，g^4，…のｐを法とする剰余があらかじめ記憶されていたがこれに換えて、Ｇ，２Ｇ，４Ｇ，…が記憶されているのが大きく異なる。更に、これにあわせて、各種の演算部の乗算も足算を行う点も異なる。

【００１０５】図１５に、通信網提供者の公開鍵作成部２１３の内部構成を示す。本図に示すように、剰余記憶部２１３１は、Ｇ，２Ｇ，４Ｇ，８Ｇ…をあらかじめ計算して記憶おり、第１実施例の乗算部１３と割算部１３４に換えて足算部２１３３を有している。また、これにより、公開鍵として、Ｅ（ＧＦ（ｐ））上の点Y_A（＝X_A Ｇ）を計算し、公開する。

【００１０６】図１６に、署名通信を行うユーザＡ側の構成を示す。本図においては、３２は２進乱数発生部であり、３４は、通信文入力部であり、これらは、先の第１実施例と異ならない。２３３はR_1 演算部であり、２進乱数発生部３２で発生させた乱数ｋ回だけ元Ｇを加えた値ｋＧを求め、その値R_1を出力する。このため、あらかじめ、２Ｇ，４Ｇ，８Ｇに対応するG_2，G_4，G_8 等を記憶している剰余記憶部２３３１、２進乱数ｋの１の立つ桁を取り出す法取り出し部２３３２、取り出した桁に対応する剰余記憶部２３３１内のG_1（ここにｉは２の乗べき）を取り出し、足し算を行う足し算部２３８３を内蔵している。

【００１０７】２３５は、Ｆ関数であり、r_2 ≡ｍ／ｘ（R_1）（ｍｏｄ ｐ)の演算によりr_2 を求める。ここにｘ（R_1）はR_1 のＸ座標値である。２３８は、求められたr_2と上記乱数ｋをもとに、演算ｓｋ≡（r_2 ＋ｓ＋１）＋r_2 x_A（ｍｏｄ ｐ)よりｓを求めるＳＫ部である。このため、ｋ－１（＝ａ）を求めるｋ－１演算部２３８１、r_2 ＋１を求めるr_2 ＋１演算部２３８２、r_2 x_A を求めるr_2 x_A 演算部２３８３、r_2 ＋１＋r_2 ＋x_A（＝ｂ）を求めるr_2 ＋１＋r_2 ＋x_A 演算部２３８４、式ｓ・ａ≡ｂ（ｍｏｄ ｐ)よりｓを求めるｓ計算部２３８５を内蔵している。

【００１０８】なお、ｍｏｄ演算の法が、ｑでなくｐであるのが第１実施例と大きく異なる。図１７は、受信例ユーザの構成図である。本図において、受信部４１、r_2 記憶部及びｓ記憶部４６は第１実施例のものと異ならない。２４７は、あらかじめＧを記憶しているＧ記憶部である。２４４は、Y_A をあらかじめ記憶しているY_A 記憶部である。

【００１０９】２４８は、r_2 とｓから（r_2 ＋ｓ＋１）／ｓを求める（r_2 ＋ｓ＋１）／ｓ演算部である。２４９は、r_2 ／ｓを求めるr_2 ／ｓ演算部である。２４１１は、Ｅ（ＧＦ（ｐ））上での演算r_2 ／ｓY_A を行うr_2 ／ｓY_A 演算部である。２４１２は、同じくＥ（ＧＦ（ｐ））上での演算（（r_2 ＋ｓ＋１）／ｓ）Ｇを行う（（r_2 ＋ｓ＋１）／ｓ）Ｇ演算部である。２４１３は、同じく、Ｅ（ＧＦ（ｐ））上での演算R_1 ＝（（ｒ

$_2$ ＋ｓ＋１）／ｓ）Ｇ＋（ｒ$_2$ ／ｓ）Ｙ$_A$ を行ってＲ$_1$ を求める演算部である。２４１４は、演算ｍ＝ｘ（Ｒ$_1$ ）ｒ$_2$ （ここに、ｘ（Ｒ$_1$ ）はＥ（ＧＦ（ｐ））上の元Ｒ$_1$ のＸ座標値）よりｍを求めるｍ演算部である。

【０１１０】このため、ｑとｒ$_2$ の大小比較を行う構成がないのも第１実施例と異なる。次に、以上の手順におけるデータそのものの処理、数式、演算を中心とした処理の流れを図１８に示す。

（１）センターによる初期設定

１０進３０桁の素数をｐとし、GF(p) 上の元の個数がpとなる楕円曲線をE とし、E(GF(p))の元を零元以外の元をG とする。このときその位数はp となる。

【０１１１】GF(p) ×GF(p) ×GF(p) からGF(p) への写像ha, hb, hcを、ha(r$_2$',s,1)=s, hc(r$_2$',s,1)=r$_2$'とし、

hb(r$_2$',s,1) ＝r$_2$' ＋s ＋1　(mod q)

で定義する。また署名式を

ha(r$_2$',s,1)k ≡ hb(r$_2$',s,1) + hc(r$_2$',s,1)x $_A$ (mod q)

で定義する。

【０１１２】センターは、システムパラメータとしてp , E(GF(p)), G, ha, hb, hc を全ユーザに公開する。なお、かかるＥ（ＧＦ（ｐ））の作成手順は、別途本願出願人が前掲の特願平６－１３４３３９号等にて開示している技術であるため、その説明は省略する。（２）署名送信を欲するユーザＡによるそのための秘密鍵の作成及びセンターが認署した公開鍵の登録。

【０１１３】ユーザＡから、メッセージ復元型署名通信を行うため、その秘密鍵を基に作成した公開鍵を通信網提供者に正しいものとして登録する要求がなされる。このため、ユーザＡは、乱数を発生させ、これを自分の秘密鍵をx $_A$ とし、対応する公開鍵を楕円曲線Ｅ（ＧＦ（Ｐ））上での演算y $_A$ ＝x $_A$ G により求め、これをセンター経由で全ユーザに公開する。

【０１１４】併せて秘密鍵ｘ$_A$ は、ユーザＡが自分のみ秘密に保持するものとする。

（３）ユーザＡによる署名の生成

ユーザＢに署名発信を行おうとするユーザＡは、以下の処理を行う。

１．乱数k を生成する。

２．２進数の乱数ｋを生成する。なお、この乱数は、各送信毎に異なる値がでるものとされている。

【０１１５】2-1)Ｅ（ＧＦ（ｐ））上で、演算Ｒ$_1$ ＝KGにより、Ｒ$_1$ を作成する。

2-2)法ｐ上の演算r$_2$ ≡ｍ ／x(Ｒ$_1$) (mod p)により、ｒ$_2$ を求める。ここに、Ｘ（Ｒ$_1$）は、Ｅ（ＧＦ（ｐ））上の点Ｒ$_1$のｘ座標値である。…(e) とする。

2-3)法ｐ上の演算sk≡(r$_2$ ＋s ＋1)＋r$_2$x $_A$ (mod p)…(f) よりs を計算する。

【０１１６】３．(r$_2$, s)をユーザＢに送信する。

（４）受信したユーザＢによるメッセージの復元

１．ユーザＡからのメッセージ（ｒ$_2$, ｓ）を受信したユーザＢは((r$_2$+s+1)/s)G+(r$_2$/s)Y $_A$ ＝Ｒ$_1$をＥ（ＧＦ（ｐ））上で計算し、Ｒ$_1$ を求める。

【０１１７】２．次いで、ｍ ＝x(Ｒ$_1$)r$_2$ を計算することによりｍ を得る。上記実施例のように構成されたメッセージ復元型署名の場合、コミットメントＲ$_1$が従来例の式(a) のように直接平文ｍ に関与するのでなく、式(e) のようにｘ座標を通して関与している。すなわち、r$_2$=F(Ｒ$_1$,ｍ)=ｍ/x(Ｒ$_1$)となる。このF 関数が

(*)1: GF(p)∋g, y$_A$, ｍ, Z$_q$ = {0,1,…,q-1} ∋t, j, e に対し、F(tG+jY $_A$, ｍ ×x(eY$_A$))及びF(tG+jY $_A$, ｍ ×x(eG))において、３変数t,j,e が２個の代数式で非置換（置き換えられ）ない。すなわち、ｍｘ（ｅＹ $_A$ ）、ｍｘ（ｅｇ）の偽造攻撃を受けない。

【０１１８】2: E(GF(p)) ∋Ｒ$_1$, G, Y$_A$, GF(p) ∋r$_2$, ｍ に対し、r$_2$=F(Ｒ$_1$,ｍ)の逆像をｍ=F $^{-1}$(Ｒ$_1$,r$_2$) で定義するとき、任意の２変数関数φ, ψに対してF $^{-1}$(Ｒ$_1$-G, r$_2$) ≠φ(ｍ,G) 及びF-1(Ｒ$_1$-Y$_A$, r$_2$) ≠ψ(ｍ,Y$_A$) となるを満たすことから、宮地らにより提案された３つの解読(recovery-equation attack using g and yA, and homomorphism attack)を回避できる。

【０１１９】また上記実施例のように構成されたメッセージ復元型署名の場合、従来例の式(b')のように署名式の係数(a,b,c) が(r$_2$',s,1) の置換という形ではなく、写像ha, hb, hcを用いて決定されている。この写像ha, hb, hcが(**)r$_2$',s をZ $_q$ の元とするとき、予め固定された少数値をのぞく全てのrr$_2$', ssに対して、次の二つの条件

1. ha(r$_2$',s,1)=ha(rr$_2$',ss,1), hc(r$_2$',s,1)=hc(rr$_2$',ss,1) のときhb(r$_2$',s,1)-ha(r$_2$',s,1)≠hb(rr$_2$',ss,1)

2. ha(r$_2$',s,1)=ha(rr$_2$',ss,1), hb(r$_2$',s,1)=hb(rr$_2$',ss,1) のときhc(r$_2$',s,1)-ha(r$_2$',s,1)≠hc(rr$_2$',ss,1)

を満たすことから、宮地らにより提案された２つの解読(signature-equation attack using g and yA)を回避できる。さらにこの署名式は従来から存在する比例関係を用いた解読に対しても、署名式が２項に分解されることがないので強い。なお、従来から存在する比例関係を用いた比例攻撃に付いては、L.Harn and Y. Xu, "Design of generalised ElGamal type digital signatureschemes based on discrete logarithm", Electron. Lett., Vol.30(1994),2025-2026.に詳しい。

【０１２０】また、上記例のような楕円曲線を用いるとG の位数が定義体GF(p) のp と等しくなるので、実施例１のようにr$_2$の値を制限するステップを付加することなく、宮地により提案された１つの解読(redundancy attack) を回避できる。また、上述の実施例はｘ座標を用いたが、これは勿論他の写像で、(*) を満たすものなら何でもよい。この際、例えばｙ座標のようにｘ座標と同じ

ように計算量が小さい写像にすることが望ましい。ha, hb, hcに関しても、上記の性質(**)をもつものなら何でもよい。またこの際、従来から存在する比例関係を用いた解読に対しても強くなるように、さらに計算量が小さい写像にすることが望ましい。

【０１２１】また、上記実施例では、定義体GF(p) のpとG の位数が等しくなるような楕円曲線を用いたが、通常の楕円曲線を用いてもよい。このときには、第１実施例のようにr_2を制限するステップを付加する必要がある。また、上記の従来例以外のどんなメッセージ復元型署名にも上記の写像を付加すると同様に解読が回避できる。

【０１２２】また、第１実施例と同じく、メッセージmに署名する代わりに、m にハッシュ関数を施したハッシュ値に対して署名し、署名をメッセージとともに送り、ハッシュ値が正しく復元されることをチェックすることで署名を確認するという署名方式として用いてのよい。また、同じく、Ｅ（ＧＦ（ｐ））でなくＥ（ＧＦ（p^r））で行ってもよい。

【０１２３】また、ユーザは、その秘密鍵等の生成を通信網提供者にしてもらうようにしてもよい。これは、適当な乱数生成器がないときに便利である。以上、本発明を実施例に基づいて説明してきたが、本発明は何も上記実施例に限定されないのは勿論である。

【０１２４】

【発明の効果】以上、説明してきたように、本発明は、法をメッセージ復元性を保ちながら、宮地らにより提案されている従来型のメッセージ復元署名に対する６つの解読法を回避することが可能となり、この一方でそのために付加される計算量も無視できる。このため、公開ディジタル通信網において、安全なメッセージ復元型署名方式を提供することが可能となり、その実用的価値は大きい。

【図面の簡単な説明】

【図１】本発明に係るメッセージ復元型署名の第１実施例の、数値や式の変換を中心とした構成、処理を示した図である。

【図２】従来の署名、認署通信の手順の一例である。

【図３】従来のメッセージ復元型署名の構成を示した図である。

【図４】従来の署名、認署通信に対する公開鍵によるrecaovry-equation 攻撃の概略手順を示した図である。

【図５】同じく、redundancy攻撃の概略図である。

【図６】本発明に係るメッセージ復元型署名通信が実施される公開ディジタル通信網の概略構成図である。

【図７】上記実施例における、通信網提供者の要部の構成図である。

【図８】同じく、署名通信を行うユーザＡの重要な処理の流れを示した図である。

【図９】同じく、署名通信を行うユーザＡ側のr_2 計算に係る部分の構成図である。

【図１０】同じく、ユーザＡ側のＳＫ部を中心とした構成図である。

【図１１】同じく、署名文を受信したユーザＢの重要な処理の流れを示した図である。

【図１２】同じく、署名文を受信したユーザＢ側の要部の構成図である。

【図１３】第１実施例の変形例として、ＧＦ（ｐ）でなくＧＦ（p^r）を使用した場合の、関数πによるＧＦ（p^r）から$Z_{p^r}=\{0, 1, \cdots, p^{r-1}\}$への変換手順を示した図である。

【図１４】本発明に係るメッセージ復元型署名通信の第２実施例が実施される公開ディジタル通信網の概略構成図である。

【図１５】上記実施例における、通信網提供者におけるＥ（ＧＦ（ｐ））上での演算を実行するための構成である。

【図１６】上記実施例における署名文の発行を行うユーザＡの構成図である。

【図１７】同じく、署名文を受信するユーザＢの構成図である。

【図１８】同じく、数、値、式の変換を中心とした構成処理を示した図である。

【符合の説明】

１　　公開ディジタル通信網提供者（各ユーザへの端末情報発行センターを兼ねる。）

２　　公開ディジタル通信網の回線

３、４、５、６、　公開ディジタル通信網に接続されたユーザ

１１　　秘密鍵作成要求受付部

１２　　秘密鍵発生部

１３　　公開鍵作成部

１４　　公開鍵公開部

１５　　秘密鍵通知形態作成部

１６　　秘密鍵通知部

３１　　r_2 制御部

３２　　２進乱数発生部

３３　　r_1 演算部

３４　　通信文入力部

３５　　ｆ関数部

３６　　ｑ関数部

３７　　排除部

３７３　　比較部

３８　　ＳＫ部

３８５　　ｓ計算部

４１　　受信部

４２　　拒絶部

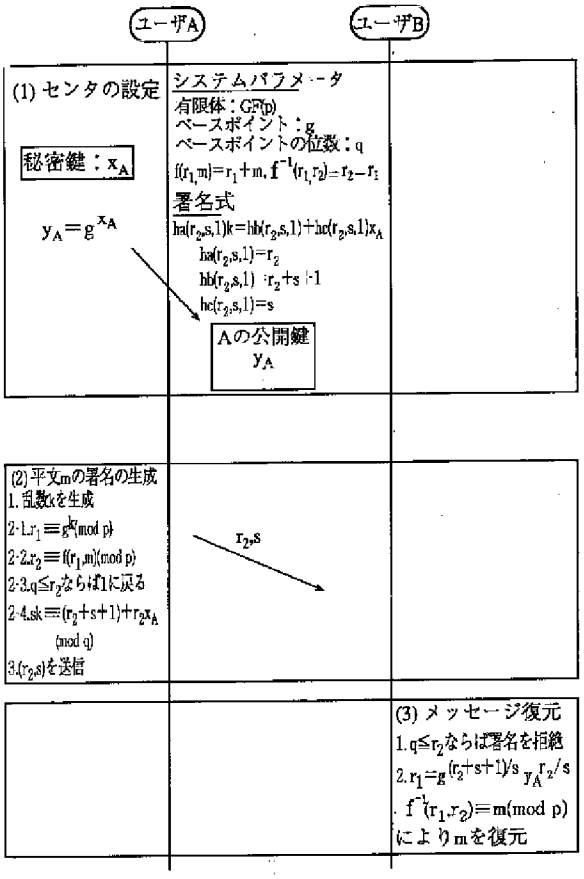
４３　　ｑ記憶部（ユーザＢ）

４４　　y_8 記憶部

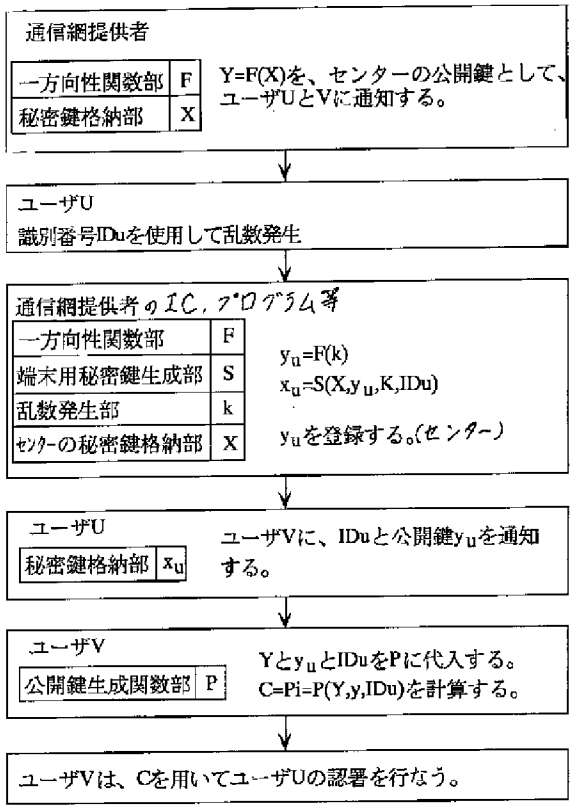
４５　　r_2 記憶部

46　s記憶部
47　g記憶部
413　$r_1 \equiv g^{(r2+s+1)/s}\, y_A{}^{R2/S} \pmod p$演算部
414　f^{-1}関数部
2131　剰余記憶部
2133　足算部
233　R_1 演算部
235　F関数部
238　SK部
244　Y_A 記憶部
2413　R_1 演算部
2414　m演算部

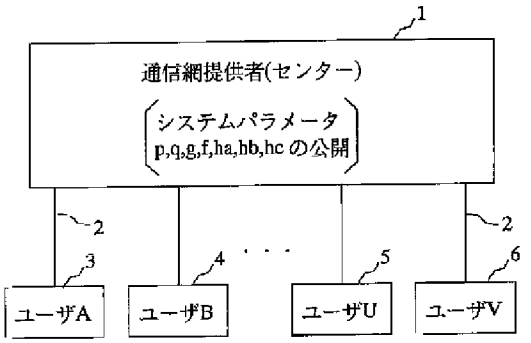
【図1】



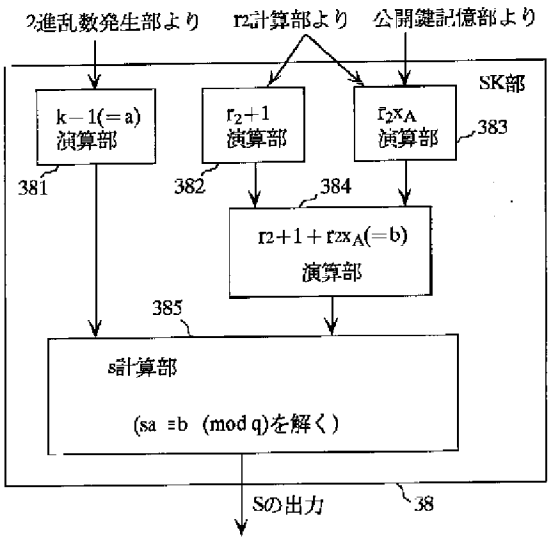
【図2】



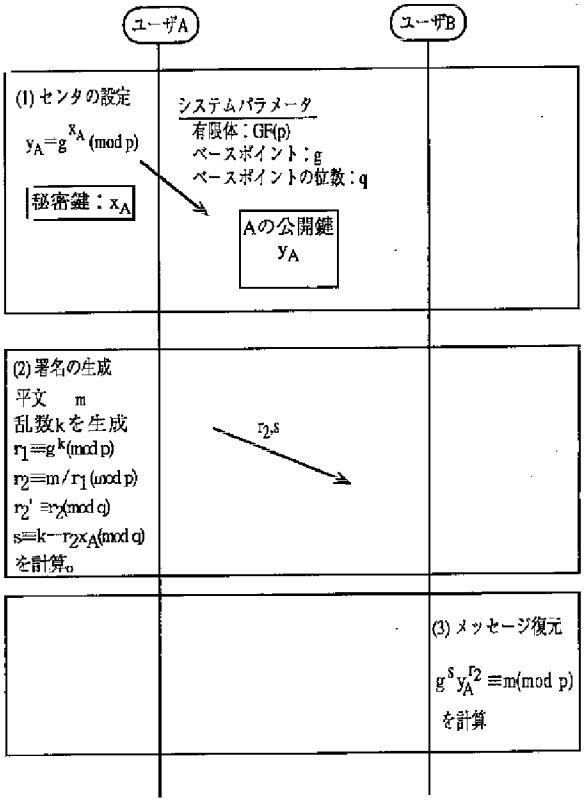
【図6】



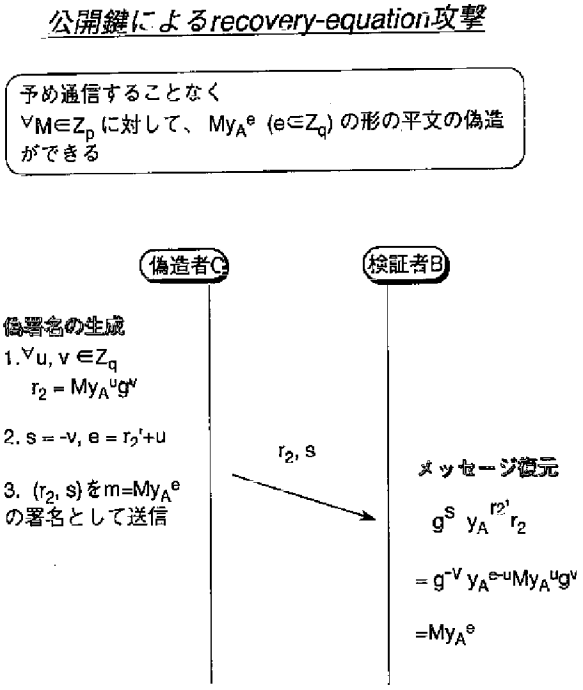
【図10】



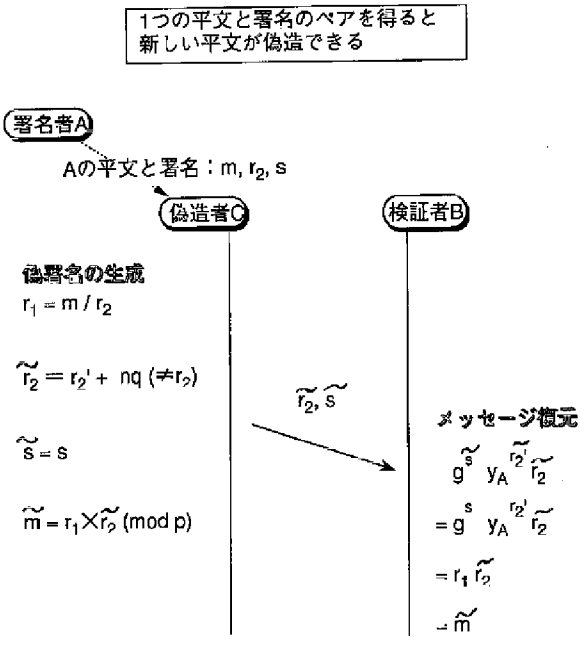
【図3】


ユーザA
ユーザB
(1) センタの設定
$y_A=g^{x_A} \pmod p$
秘密鍵：x_A
システムパラメータ
有限体：GF(p)
ベースポイント：g
ベースポイントの位数：q
Aの公開鍵
y_A
(2) 署名の生成
平文　m
乱数kを生成
$r_1 \equiv g^k \pmod p$
$r_2 \equiv m / r_1 \pmod p$
$r_2' \equiv r_2 \pmod q$
$s \equiv k - r_2 x_A \pmod q$
を計算。
r_2, s
(3) メッセージ復元
$g^s y_A^{r_2} \equiv m \pmod p$
を計算

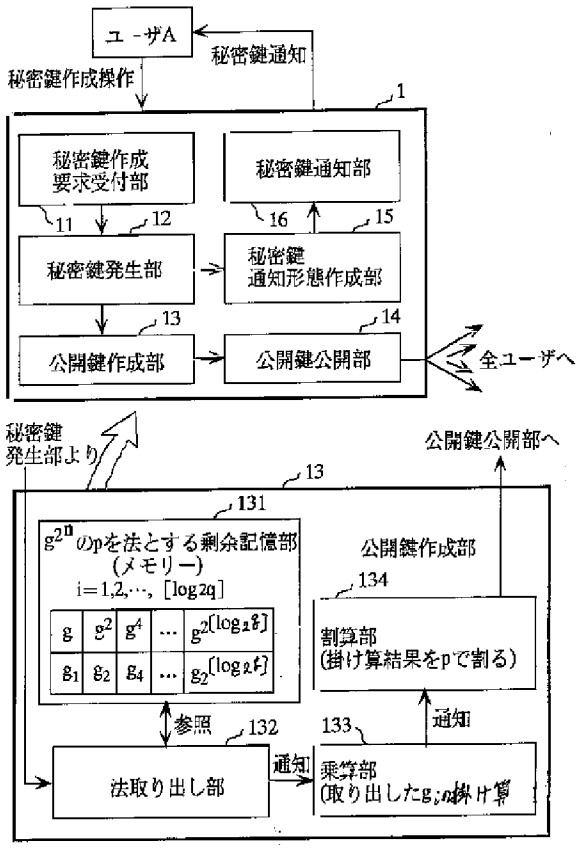
【図4】


公開鍵によるrecovery-equation攻撃
予め通信することなく
$\forall M \in Z_p$ に対して、My_A^e $(e \in Z_q)$ の形の平文の偽造ができる
偽造者C
検証者B
偽署名の生成
1. $\forall u, v \in Z_q$
$r_2 = My_A^u g^v$
2. $s = -v, e = r_2' + u$
3. (r_2, s)をm=My_A^eの署名として送信
r_2, s
メッセージ復元
$g^s y_A^{r_2'} r_2$
$= g^{-v} y_A^{e-u} My_A^u g^v$
$= My_A^e$

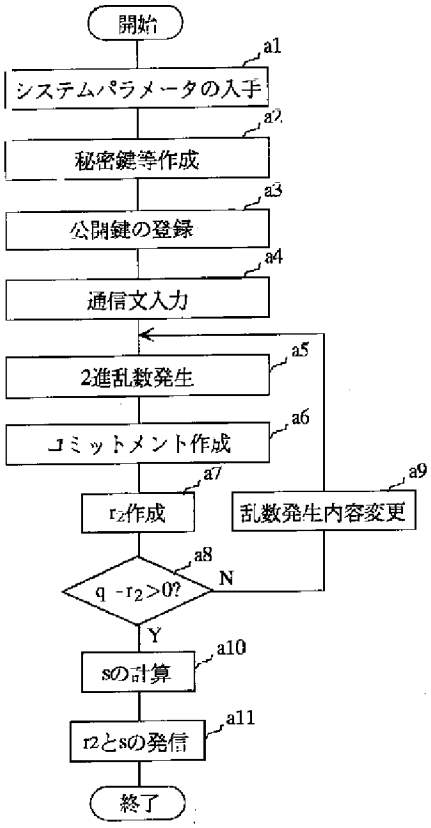
【図5】


redundancy攻撃
1つの平文と署名のペアを得ると新しい平文が偽造できる
署名者A
Aの平文と署名：m, r_2, s
偽造者C
検証者B
偽署名の生成
$r_1 = m / r_2$
$\tilde{r_2} = r_2' + nq \ (\neq r_2)$
$\tilde{s} = s$
$\tilde{m} = r_1 \times \tilde{r_2} \pmod p$
$\tilde{r_2}, \tilde{s}$
メッセージ復元
$g^{\tilde{s}} y_A^{r_2'} \tilde{r_2}$
$= g^s y_A^{r_2'} \tilde{r_2}$
$= r_1 \tilde{r_2}$
$= \tilde{m}$

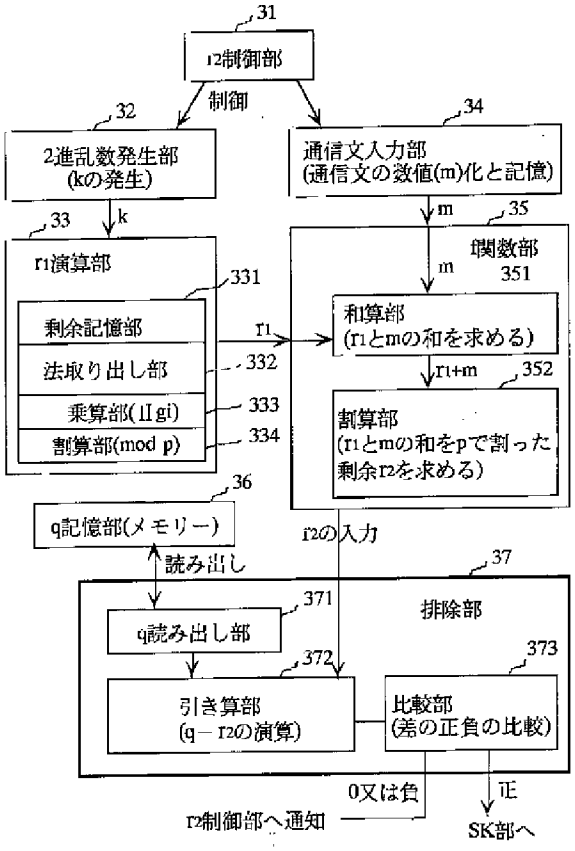
【図7】


ユーザA
秘密鍵通知
秘密鍵作成操作
1
秘密鍵作成要求受付部
秘密鍵通知部
11
12
16
15
秘密鍵発生部
秘密鍵通知形態作成部
13
14
公開鍵作成部
公開鍵公開部
全ユーザへ
秘密鍵発生部より
公開鍵公開部へ
13
131
g^{2^n}のpを法とする剰余記憶部（メモリー）
i=1,2,…, [log2q]
g g^2 g^4 … $g^{2^{[\log_2 q]}}$
g_1 g_2 g_4 … $g_2^{[\log_2 q]}$
公開鍵作成部
134
割算部（掛け算結果をpで割る）
参照
132
133
通知
法取り出し部
通知
乗算部（取り出したg_i^n掛け算

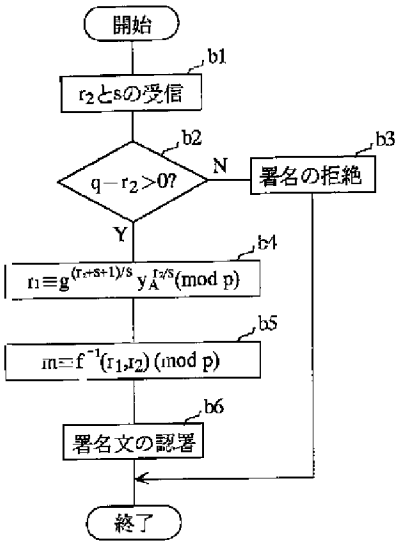
【図８】


開始
a1
システムパラメータの入手
a2
秘密鍵等作成
a3
公開鍵の登録
a4
通信文入力
a5
2進乱数発生
a6
コミットメント作成
a7
r2作成
a9
乱数発生内容変更
a8
q −r2>0?
N
Y
a10
sの計算
a11
r2とsの発信
終了

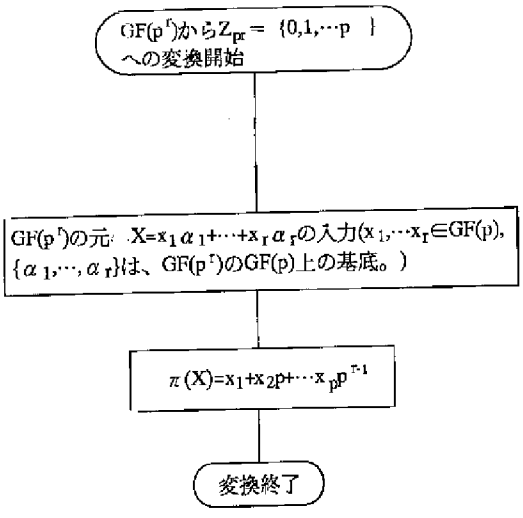
【図９】


31
r2制御部
制御
32
2進乱数発生部
(kの発生)
34
通信文入力部
(通信文の数値(m)化と記憶)
k
m
33
r1演算部
35
f関数部
m
351
331
剰余記憶部
r1
和算部
(r1とmの和を求める)
法取り出し部
332
r1+m
352
乗算部(Πgi)
333
割算部
(r1とmの和をpで割った
剰余r2を求める)
割算部(mod p)
334
36
q記憶部(メモリー)
r2の入力
読み出し
37
排除部
371
q読み出し部
373
372
引き算部
(q−r2の演算)
比較部
(差の正負の比較)
0又は負
正
r2制御部へ通知
SK部へ

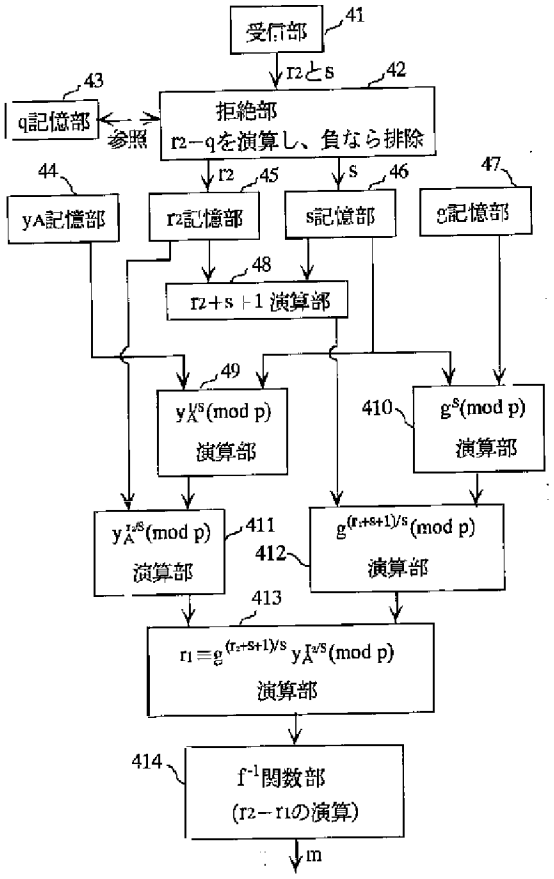
【図１１】


開始
b1
r2とsの受信
b2
q−r2>0?
N
b3
署名の拒絶
Y
b4
r1≡g^((r2+s+1)/s) y_A^(r2/s) (mod p)
b5
m=f^-1(r1,r2) (mod p)
b6
署名文の認署
終了

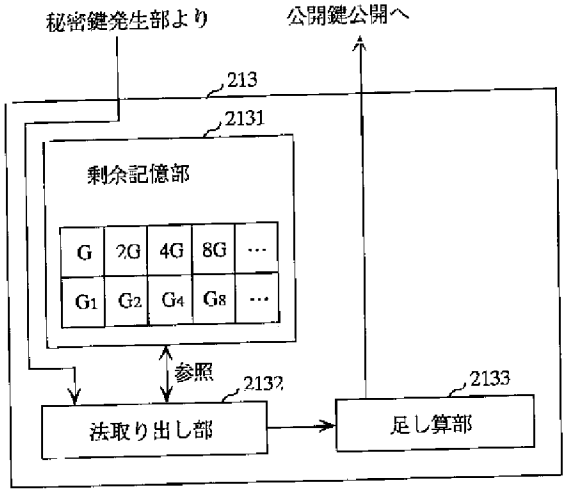
【図１３】


GF(p^r)からZ_pr = {0,1,…p }
への変換開始
GF(p^r)の元 X=x1α1+…+xrαrの入力(x1,…xr∈GF(p),
{α1,…,αr}は、GF(p^r)のGF(p)上の基底。)
π(X)=x1+x2p+…xrp^r-1
変換終了

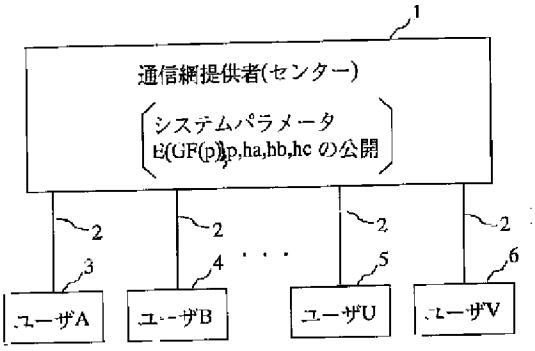
【図１２】



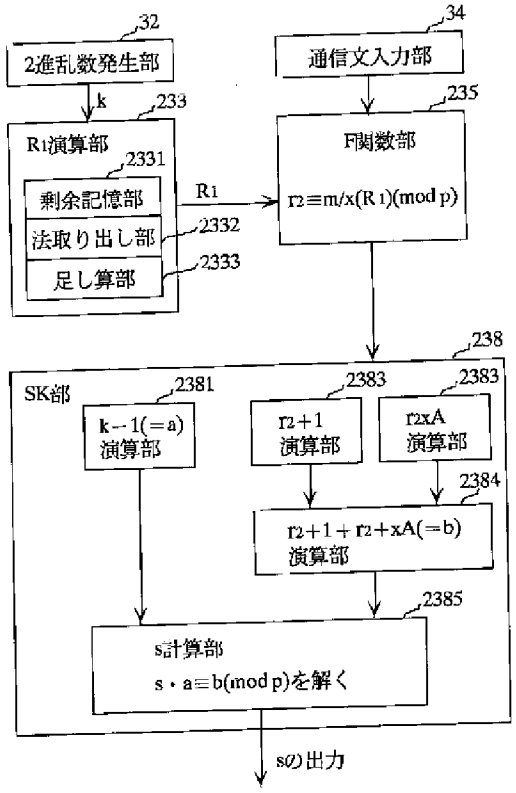
【図１３】



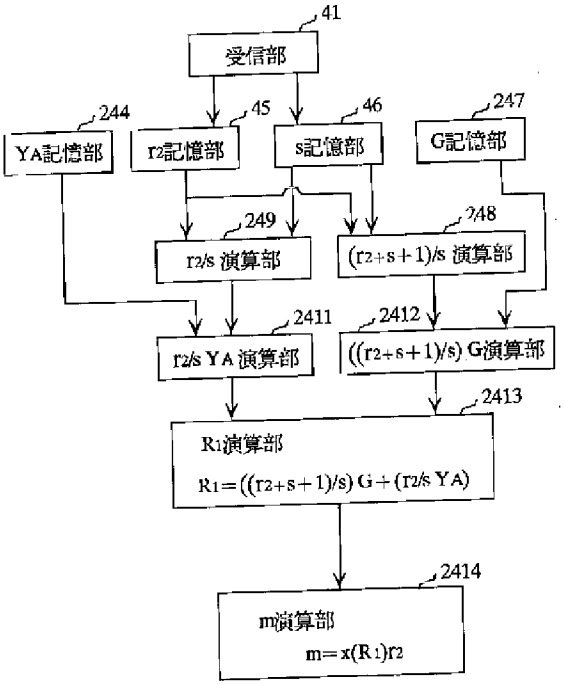
【図１４】



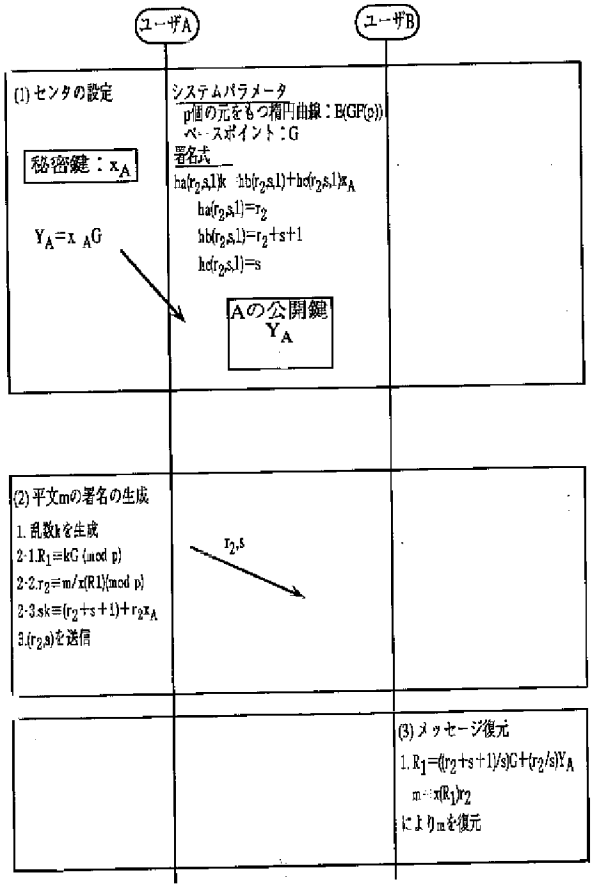
【図１６】



【図１７】


41
受信部
244
YA記憶部
45
r2記憶部
46
s記憶部
247
G記憶部
249
r2/s 演算部
248
(r2+s+1)/s 演算部
2411
r2/s YA 演算部
2412
((r2+s+1)/s) G演算部
2413
R1演算部
R1=((r2+s+1)/s) G+(r2/s YA)
2414
m演算部
m=x(R1)r2

【図１８】


ユーザA
ユーザB
(1) センタの設定
システムパラメータ
p値の元をもつ楕円曲線：E(GF(p))
ベースポイント：G
秘密鍵：xA
署名式
ha(r2,s,1)k=hb(r2,s,1)+hc(r2,s,1)xA
ha(r2,s,1)=r2
hb(r2,s,1)=r2+s+1
hc(r2,s,1)=s
YA=xAG
Aの公開鍵
YA
(2) 平文mの署名の生成
1. 乱数kを生成
2-1.R1=kG (mod p)
2-2.r2=m/x(R1)(mod p)
2-3.sk=(r2+s+1)+r2xA
3.(r2,s)を送信
r2,s
(3) メッセージ復元
1. R1=((r2+s+1)/s)G+(r2/s)YA
m=x(R1)r2
によりmを復元